Joint Publication 2-0

Joint Intelligence

22 June 2007

This revised edition of JP 2-0, *Joint Intelligence*, reflects the current guidance for conducting joint and multinational intelligence activities across the range of military operations. This vital keystone publication forms the core of joint intelligence doctrine and lays the foundation for our forces' ability to fully integrate operations, plans, and intelligence into a cohesive team. The overarching constructs and principles contained in this publication provide a common perspective from which to plan and execute joint intelligence operations in cooperation with our multinational partners, other US Government agencies, and intergovernmental and nongovernmental organizations.

As our Nation continues into the 21st century, joint intelligence organizations and capabilities will continue to evolve as our forces transform to meet emerging challenges. The guidance in this publication will enable current and future leaders of the Armed Forces of the United States to organize, train, and execute worldwide missions to counter the threats posed by adaptive adversaries.

I encourage all leaders to study and understand the doctrinal concepts and principles contained in this publication and to teach these to your subordinates. Only then will we be able to fully exploit the remarkable military potential inherent in our joint teams. To that end, I request you ensure the widest possible distribution of this keystone joint publication. I further request that you actively promote the use of all joint publications at every opportunity.

PETER PACE
General, United States Marine Corps
Chairman
of the Joint Chiefs of Staff

PREFACE

1. Scope

This publication is the keystone document of the joint intelligence series. It provides fundamental principles and guidance for intelligence support to joint operations and unified action.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff. It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations and provides the doctrinal basis for interagency coordination and for US military involvement in multinational operations. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations, education, and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

3. Application

a. Joint doctrine established in this publication applies to the joint staff, commanders of combatant commands, subunified commands, joint task forces, subordinate components of these commands, and the Services.

b. The guidance in this publication is authoritative; as such, this doctrine will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the Chairman of the Joint Chiefs of Staff, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with US law, regulations, and doctrine.

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 2-0
DATED 9 MARCH 2000

- **Establishes and discusses principles of joint intelligence**
- **Identifies the intelligence disciplines and describes their related subcategories, sources, and capabilities**
- **Provides a methodology for assigning confidence levels to the analytic conclusions contained in intelligence products**
- **Explains the use of "red teams" to support intelligence analysis and course of action wargaming**
- **Explains the roles and responsibilities of the Director of National Intelligence and the Under Secretary of Defense for Intelligence**
- **Describes the intelligence-related responsibilities of commanders and their intelligence staffs**
- **Discusses the missions and functions of the joint intelligence operations centers at Department of Defense and combatant command levels**
- **Discusses intelligence support to planning, executing, and assessing joint operations**
- **Establishes and discusses principles for interagency intelligence collaboration and multinational intelligence sharing**
- **Replaces the term "joint intelligence preparation of the battlespace" with the term "joint intelligence preparation of the operational environment"**
- **Discusses a "systems perspective of the operational environment"**
- **Promulgates a significant modification to the definition of intelligence that describes the term as both a product and activity**
- **Establishes new definitions for the terms "biometric," "biometrics," "dynamic threat assessment," "joint intelligence operations center," "obstacle intelligence," and "red team"**

Intentionally Blank

TABLE OF CONTENTS

GLOSSARY

FIGURE

Intentionally Blank

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Discusses the Nature of Intelligence**
- **Covers the Principles of Joint Intelligence**
- **Discusses Intelligence Organizations and Responsibilities**
- **Describes Intelligence Support to Planning, Executing, and Assessing Joint Operations**
- **Covers Joint, Interagency, and Multinational Intelligence Sharing and Cooperation**

Introduction

Intelligence oversight and the production and integration of intelligence in military operations are inherent responsibilities of command.

Information is of greatest value when it contributes to or shapes the commander's decision-making process by providing reasoned insight into future conditions or situations. This may occur as a result of its association with other information already received or when it is considered in the light of experience already possessed by the recipient of the information. Information on its own is a fact or a series of facts that may be of utility to the commander, but when related to other information already known about the operational environment and considered in the light of past experience regarding an adversary, it gives rise to a new set of facts "**intelligence**." The relating of one set of information to another or the comparing of information against a database of knowledge already held and the drawing of conclusions by an intelligence analyst, is the foundation of the process by which intelligence is produced. Ultimately, intelligence has two critical features that make it different from information. **Intelligence allows anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating the differences in available courses of action (COAs).**

The primary function of joint intelligence is to provide information and assessments to facilitate accomplishment of the mission.

The **purposes of joint intelligence** that guide the intelligence directorate of a joint staff (J-2) staff and those of supporting organizations are: inform the commander; identify, define, and nominate objectives; support the planning and execution of operations; counter adversary deception and surprise; support friendly deception efforts; and assess the effects of operations on the adversary**.**

The Joint Intelligence Process

The joint intelligence process provides the basis for common intelligence terminology and procedures, and consists of six interrelated categories of intelligence operations.

Intelligence operations are wide-ranging activities conducted by intelligence staffs and organizations for the purpose of providing commanders and national-level decision makers with relevant, accurate, and timely intelligence. The six categories of intelligence operations are: planning and direction; collection; processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback.

Planning and Direction. Intelligence planning for rapid response to possible crises occurs well ahead of time as part of a command's overall joint operation planning process. The most likely threat scenarios are used as the core of this planning effort, which includes determining the personnel, equipment, and intelligence architecture essential for generic support to force deployments. When a particular crisis situation unfolds, planners develop an operation order (OPORD).

Collection. Collection includes those activities related to the acquisition of data required to satisfy the requirements specified in the collection plan. Collection operations management involves the direction, scheduling, and control of specific collection platforms, sensors and human intelligence sources and alignment processing, exploitation, and reporting resources with planned collection.

Processing and Exploitation. During processing and exploitation, raw collected data is converted into forms that can be readily used by commanders, decision makers at all levels, intelligence analysts and other consumers.

Analysis and Production. During analysis and production, intelligence is produced from the information gathered by the collection capabilities assigned or attached to the joint force and from the refinement and compilation of intelligence received from subordinate units and external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that will satisfy the commander's priority intelligence requirements or request for information.

Dissemination and Integration. During dissemination and integration, intelligence is delivered to and used by the consumer. Dissemination is facilitated by a variety of means. The means must be determined by the needs of the user and the implications and criticality of the intelligence.

Evaluation and Feedback. During evaluation and feedback, intelligence personnel at all levels assess how well each of the various types of intelligence operations are being performed.

Intelligence and the Levels of War

All levels of war have corresponding levels of intelligence operations.

The construct of **strategic, operational, and tactical levels of intelligence** aids joint force commanders (JFCs) and their J-2s in visualizing the flow of intelligence from one level to the next. This construct facilitates the allocation of required collection, analytical, and dissemination resources and permits the assignment of appropriate intelligence tasks to national, theater, component, and supporting intelligence elements. The different categories of intelligence production support each level of intelligence, both horizontally and vertically.

Intelligence operations at all levels must support the commander. Strategic intelligence operations provide continuity and depth of coverage even while the joint force is deploying. During campaign planning, strategic and operational intelligence operations focus on providing to the JFC information required to identify the adversary's centers of gravity (COGs), COAs, and high-value targets. During execution, operational intelligence operations provide the JFC with relevant, timely, and accurate intelligence relating to the accomplishment of campaign or major operation objectives.

Levels of command, size of units, types of equipment, or types of forces or components are not associated with a particular level of intelligence operations. Operational and tactical intelligence operations, in conjunction with appropriate assessments, provide the JFC the information required to identify adversary critical vulnerabilities COGs and critical nodes for the optimum application of all available resources, thereby allowing the JFC to most effectively employ the joint task force's capabilities.

Intelligence and the Range of Military Operations

Intelligence operations continue throughout the range of military operations.

Joint Publication (JP) 3-0, *Joint Operations,* divides the range of military operations into three major categories: military engagement, security cooperation, and deterrence; crisis response and limited contingency operations; and major operations and campaigns.

Military Engagement, Security Cooperation, and Deterrence Operations. Maintaining a forward presence enables US forces to gain regional familiarity and develop a common understanding of important cultural, historical, interpersonal, and social differences. Activities such as professional military exchanges, forward basing, and cooperative relationships with multinational partners enhance US forces' ability to shape potential military engagement, security cooperation, and deterrence operations, gain an understanding of multinational tactics and procedures, enhance information sharing, and establish mutual support with host country nationals. Intelligence support is essential to activities such as emergency preparedness, arms control verification, combating terrorism, counterdrug operations, enforcement of sanctions and exclusion zones, ensuring freedom of navigation and overflight, nation assistance, protection of shipping, shows of force, and support to insurgency and counterinsurgency operations.

Crisis Response and Limited Contingency Operations. Intelligence provides assessments that help the JFC decide which forces to deploy; when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission. The intelligence requirements in support of crisis response and limited contingency operations such as noncombatant evacuation operations, peace operations, foreign humanitarian assistance, recovery operations, consequence management actions associated with chemical, biological, radiological, nuclear, and high-yield explosives, strikes and raids, homeland defense, and civil support are similar to those required during major operations.

Major Operations and Campaigns. Intelligence identifies enemy capabilities, helps identify the COGs, projects probable COAs, and assists in planning friendly force employment. By determining the symmetries and

asymmetries between friendly and enemy forces, intelligence assists the JFC and operational planners in identifying the best means to accomplish the joint force mission.

Principles of Joint Intelligence

Perspective.

Perspective — Intelligence analysts must seek to understand the adversary's thought process, and should develop and continuously refine their ability to think like the adversary. They must offer this particular expertise for the maximum benefit of the JFC, joint staff elements, and component commands planning, execution, and assessment. The JFC should require the J-2 to assess all proposed actions from the following perspective: "How will the adversary likely perceive this action, and what are the adversary's probable responses?"

Synchronization.

Synchronization — Intelligence must be synchronized with operations and plans in order to provide answers to intelligence requirements in time to influence the decision they are intended to support. Intelligence synchronization requires that all intelligence sources and methods be applied in concert with the operation plan (OPLAN) and operation order (OPORD). OPLAN and OPORD requirements therefore constitute the principal driving force that dictates the timing and sequencing of intelligence operations.

Integrity.

Integrity — Intellectual integrity must be the hallmark of the intelligence profession. It is the cardinal element in intelligence analysis and reporting, and the foundation on which credibility with the intelligence consumer is built. Integrity requires adherence to facts and truthfulness with which those facts are interpreted and presented. Moral courage is required to remain intellectually honest and to resist the pressure to reach intelligence conclusions that are not supported by facts. Intelligence concerning a situation is one of the factors in determining policy, but policy must not determine the intelligence.

Unity of Effort.

Unity of Effort — Unity of effort – coordination through cooperation and common interests to achieve a desired end state – is essential to effective joint intelligence operations. Unity of effort is facilitated by centralized planning and direction and decentralized execution of intelligence operations, which enables JFCs to apply all available intelligence, surveillance, and reconnaissance assets wisely, efficiently, and effectively.

Prioritization. **Prioritization** — Because operational needs for intelligence often exceed intelligence capabilities, prioritization of collection and analysis efforts and intelligence, surveillance, and reconnaissance (ISR) resource allocation are vital aspects of intelligence planning. Prioritization offers a mechanism for addressing requirements and effectively managing risk by identifying the most important tasks and applying available resources against those tasks.

Excellence. **Excellence** — Producers of intelligence should constantly strive to achieve the highest possible level of excellence in their products. The quality of intelligence products is paramount to the intelligence professional's ability to attain and maintain credibility with intelligence consumers. To achieve the highest standards of excellence, intelligence must be: **anticipatory, timely, accurate, usable, complete, relevant, objective, and available.**

Prediction. **Prediction** — Although intelligence must identify and assess the full range of adversary capabilities, it is most useful when it focuses on the future and adversary intentions. JFCs require and expect timely intelligence estimates that accurately identify adversary intentions, support offensive and/or defense operations, and predict adversary future COAs in sufficient detail as to be actionable.

Agility. **Agility** — Agility is the ability to shift focus nearly instantaneously and bring to bear the skill sets necessary to address the new problem at hand while simultaneously continuing critical preexisting work. Intelligence structures, methodologies, databases, products, and personnel must be sufficiently agile and flexible to meet changing operational situations, needs, priorities, and opportunities.

Collaboration. **Collaboration** — By its nature intelligence is imperfect (i.e., everything cannot be known, analysis is vulnerable to deception, and information is open to alternative interpretations). The best way to avoid these obstacles and achieve a higher degree of fidelity is to consult with, and solicit the opinions of, other analysts and experts, particularly in external organizations.

Fusion. **Fusion** — Fusion is the process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity. It draws on the complementary strengths of all intelligence disciplines, and relies on an all-source approach to intelligence collection and analysis.

Intelligence Organizations and Responsibilities

A wide variety of intelligence organizations exist at the national and theater levels that are capable of providing support to joint operations.

During most joint operations, JFCs will require not only military intelligence, but also intelligence on nonmilitary aspects of the operational environment such as economic, informational, social, political, diplomatic, biographic, human factors, and other types of intelligence. Equally important is knowledge of how all these aspects interrelate to form a systems perspective of the adversary and other relevant aspects of the operational environment. In order to efficiently exploit the wide range of knowledge and other intelligence expertise resident in both Department of Defense (DOD) and non-DOD members of the intelligence community (IC), **JFCs and their J-2s should understand the national intelligence structure** as well as respective roles and responsibilities of theater and national intelligence organizations.

Defense and Joint Intelligence Organizations

Defense Joint Intelligence Operations Center (DJIOC). The DJIOC is the lead DOD intelligence organization responsible for integrating and synchronizing military intelligence and national intelligence capabilities. It plans, prepares, integrates, directs, synchronizes, and manages continuous, full-spectrum DOD intelligence operations in support of the combatant commands. The DJIOC collaborates with United States Strategic Command's (USSTRATCOM's) Joint Functional Component Command-Intelligence Surveillance, and Reconnaissance (JFCC-ISR) and Director of National Intelligence (DNI) representatives to formulate and recommend to the Chairman of the Joint Chiefs of Staff, for Secretary of Defense action, solutions for deconflicting combatant command requirements for national intelligence resources, and ensures an integrated response to their needs. It ensures that joint force crisis-related and time-sensitive intelligence requirements are tasked to the appropriate Service, combatant command or national agency, when the requirements cannot be satisfied by assigned or attached assets.

Combatant Command Joint Intelligence Operations Centers (JIOCs). The combatant command JIOCs are the primary intelligence organizations providing support to joint forces at the operational and tactical levels. The JIOC integrates the capabilities of DNI, Service, combat support agency, and combatant command intelligence assets to coordinate intelligence planning, collection management, analysis and support. The JIOC construct seamlessly combines all intelligence functions, disciplines, and operations into a single organization, ensures the availability of all sources of information from both combatant command and national intelligence

resources, and fully synchronizes and integrates intelligence with operation planning and execution.

Joint Task Force Joint Intelligence Support Elements. At the discretion of a subordinate JFC, a joint task force (JTF) joint intelligence support element (JISE) may be established during the initial phases of an operations to augment the subordinate joint force J-2 element. Under the direction of the joint force J-2, a JTF JISE normally manages the intelligence collection, production, and dissemination for a joint force.

Intelligence Support to Planning Joint Operations

Operation planning occurs in a networked, collaborative environment, which requires iterative dialogue among senior leaders, concurrent and parallel plan development, and collaboration across multiple planning levels.

Intelligence planning supports joint operation planning and results in **three major products:** a Defense Intelligence Agency produced dynamic threat assessment, a combatant command J-2 produced annex B (Intelligence), and a national intelligence support plan (NISP) produced by the DJIOC. Together the annex B and the NISP integrate and synchronize the intelligence capabilities of the combatant command and the DOD portion of the IC to answer the commander's focused intelligence needs to help achieve the JFC's objectives.

The DJIOC, USSTRATCOM's JFCC-ISR, and combatant command JIOCs are the focal points for intelligence planning designed to synchronize the efforts of the DOD portion of the IC and to orchestrate the broader IC effort with the theater plan. Intelligence planning provides a comprehensive methodology for integrating intelligence into plans, and focusing IC capabilities on satisfying combatant command intelligence requirements. Intelligence planning should also include collection and production requirements related to critical infrastructure protection. The intelligence planning process is conducted in four phases that correspond to the four joint planning functions discussed in JP 5-0, *Joint Operations Planning*: strategic guidance, concept development, plan development, and plan assessment.

Intelligence Support to Executing Joint Operations

Execution begins when the President decides to use a military option to resolve a crisis.

Only the President or Secretary of Defense can authorize the Chairman of the Joint Chiefs of Staff to issue an execute order (EXORD). The EXORD directs the supported commander to initiate military operations, defines the time to initiate operations, and conveys guidance not provided earlier. The Chairman of the Joint Chiefs of Staff monitors the deployment and employment of forces, acts to resolve shortfalls, and directs action needed to ensure successful

completion of military operations. Execution continues until the operation is terminated or the mission is accomplished or revised. Execution consists of mobilization, deployment, employment, sustainment, redeployment, and demobilization activities. **Intelligence support is crucial to all aspects of execution.** Immediate, precise, and persistent intelligence support to force employment is a particularly important prerequisite for military success throughout all phases of a joint operation (i.e., shaping, deterrence, seizing the initiative, dominance, stabilization, and enabling civil authority) regardless of how the battle evolves. JIOCs must be familiar with specific phasing arrangements of each command OPLAN because the phasing may differ for specific types of operations. During execution, intelligence must stay at least one step ahead of operations and not only support the current phase of the operation, but also simultaneously lay the informational groundwork required for subsequent phases. Execution of joint operations requires optimizing the use of limited ISR assets and maximizing the efficiency of intelligence production resources and is the ultimate test of the efficacy of intelligence support planning.

Intelligence Support to Assessing Joint Operations

Continuous and timely assessment are essential to measure progress of the joint force toward mission accomplishment.

Commanders continuously assess the operational environment and the progress of operations, and then compare them to their initial vision and intent. Normally, the joint force J-2 assists the operations directorate in coordinating assessment activities. The joint force J-2, through the combatant command JIOC, helps the commander by assessing adversary capabilities, vulnerabilities and intentions, and monitoring the numerous aspects of the operational environment that can influence the outcome of operations. The J- 2 also helps the commander and staff decide what aspects of the operational environment to measure and how to measure them to determine progress toward accomplishing a task, creating an effect, or achieving an objective. Intelligence personnel use the joint intelligence preparation of the operational environment process to provide JFCs and their staffs with a detailed understanding of the adversary and other aspects of the operational environment.

Intelligence personnel in the combatant command JIOC provide objective assessments to planners that gauge the overall impact of military operations against adversary forces as well as provide an assessment of likely adversary reactions and counteractions. The combatant commander (CCDR) and subordinate JFCs should establish an assessment management system that leverages and synergizes the expertise of operations and intelligence staffs.

Joint, Interagency, and Multinational Intelligence Sharing and Cooperation

The success of joint and multinational operations and interagency coordination hinges upon timely and accurate information and intelligence sharing.

A JFC must be capable of coordinating the actions of people, organizations, and resources at great distances among diverse participants, such as allies and coalition partners, other government agencies, nongovernmental organizations (NGOs), and state and local authorities. To prevail, the JFC's decision-making and execution cycles must be consistently faster than the adversary's and be based on better information. Being faster and better requires having unfettered access to the collection, processing, and dissemination of information derived from all available sources. **Information sharing, cooperation, collaboration and coordination are enabled by an intelligence and information sharing environment that fully integrates joint, multinational, and interagency partners in a collaborative enterprise.** This type of collaborative intelligence sharing environment must be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time. The architecture supporting this type of environment must be dynamic, flexible, and capable of providing multinational partners and interagency participants rapid access to appropriate data. It must facilitate the capability of the national and defense intelligence communities to focus on supporting the JFC and subordinate joint force components and to integrate support from non-DOD agencies and NGOs as needed. The intelligence sharing architecture is configured to provide the baseline data needed to support commanders at all levels. CCDRs are responsible for the intelligence sharing architecture for their commands. For contingency operations, subordinate JFCs, supported by their joint force J-2s, are responsible for establishing the joint force intelligence architecture required to accomplish the assigned mission.

CONCLUSION

This document is the keystone document of the joint intelligence series. This publication provides fundamental principles and guidance for intelligence support to joint operations and unified action.

CHAPTER I
THE NATURE OF INTELLIGENCE

"By 'intelligence' we mean every sort of information about the enemy and his country — the basis, in short, of our own plans and operations."

Clausewitz
On War, 1832

1. Introduction

Intelligence oversight and the production and integration of intelligence in military operations are inherent responsibilities of command. These responsibilities are performed at every echelon of command and across the range of military operations. Today's technology enables joint force and component commanders and their staffs to access in near-real-time, very large amounts of information relating to every aspect of the operational environment — the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Information will be available throughout the joint force covering an extremely wide range of matters relating to friendly, neutral, and enemy forces and the civilian populace. There will also be an equally large volume of information concerning weather, terrain, cultural influences, and other aspects of the operational environment. This mass of information, when subjected to an analytical process, can be distilled into intelligence to support a predictive estimate of adversary capabilities and intentions. It is this predictive nature of intelligence that distinguishes it from the mass of other information available to the commander.

a. Information is of greatest value when it contributes to or shapes the commander's decision-making process by providing reasoned insight into future conditions or situations. This may occur as a result of its association with other information already received or when it is considered in the light of experience already possessed by the recipient of the information. For example, raw data by itself has relatively limited utility. However, when data is collected from a sensor and processed into an intelligible form, it becomes information and gains greater utility. Information on its own is a fact or a series of facts that may be of utility to the commander, but when related to other information already known about the operational environment and considered in the light of past experience regarding an adversary, it gives rise to a new set of facts, which may be termed "**intelligence**." The relating of one set of information to another or the comparing of information against a database of knowledge already held and the drawing of conclusions by an intelligence analyst, is the foundation of the process by which intelligence is produced. The relationship between data, information, and intelligence is graphically depicted at Figure I-1. Ultimately, intelligence has two critical features that make it different from information. Intelligence allows anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating the differences in available courses of action (COAs).

b. Intelligence provides the commander with a threat assessment based on an analysis of the full range of adversary capabilities and a prediction of the adversary's likely intention. With predictive, accurate, and relevant intelligence, commanders may gain the critical advantage of getting inside the adversary's decision-making cycle, improving insight into how the adversary will act or react. The

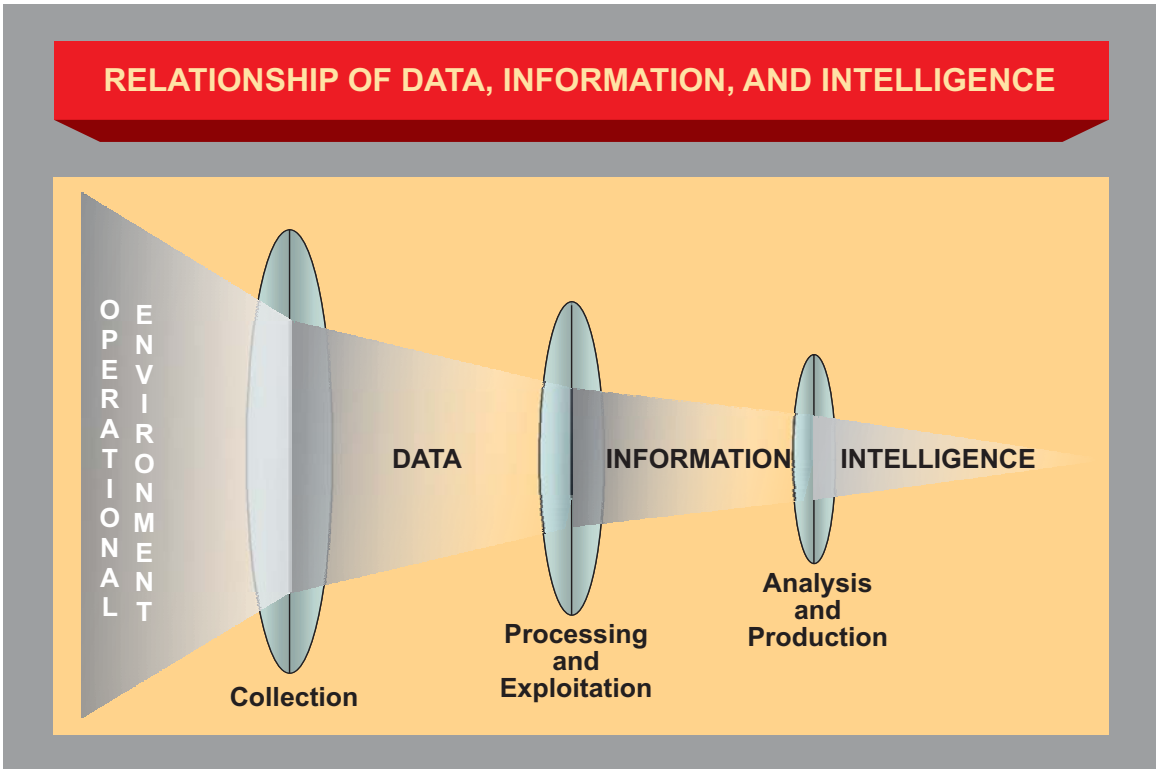


Figure I-1. Relationship of Data, Information, and Intelligence

commander can therefore formulate plans based on this knowledge and thus decrease the risks inherent in military operations and increase the likelihood of success.

c. Intelligence is not an exact science; there will always be some uncertainty in the minds of intelligence analysts as they assess the adversary, and the commander and staff as they plan and execute operations. Likewise, intelligence, as the synthesis of quantitative analysis and qualitative judgment, is rarely unequivocal and is therefore subject to competing interpretation. It is therefore important that intelligence analysts provide an estimate of the degree of confidence they have in their analytic conclusions. Such estimates of analytic confidence help intelligence consumers decide how much weight to place on intelligence assessments when making a decision. One methodology intelligence personnel may use to assign a confidence level to their analytic conclusions or intelligence assessments is discussed in Appendix A, "Intelligence Confidence Levels."

d. Intelligence includes organizations, processes, and products and involves the collection, processing, exploitation, analysis, and dissemination of information important to decision makers. Intelligence, however, is not an end in itself. For intelligence to have utility, it requires users. Thus, an examination of whether or not intelligence is effective or influential not only depends on the intelligence organizations, processes, and products, but must also consider the users. Explicit user requirements, properly communicated to intelligence agencies, initiate the intelligence collection process. Intelligence products provide users with the information that has been collected and analyzed based on their requirements.

2. The Purposes of Joint Intelligence

The primary function of joint intelligence is to provide information and assessments to facilitate accomplishment of the mission. This function is supported by more-specific "purposes of joint intelligence" (described below) to guide the intelligence directorate of a joint staff (J-2) staff and those of supporting organizations (see Figure I-2).

a. **Inform the Commander.** The J-2 directly supports the joint force commander (JFC) in planning, transitioning from planning to operations, and conducting assessment of those operations. The J-2 analyzes the adversary and other relevant aspects of the operational environment, and produces threat assessments on a continuing basis to support the commander in creating and/or exploiting opportunities to accomplish friendly force objectives. To maintain the initiative, the JFC will seek to understand and potentially influence the adversary's decision-making process (i.e., the JFC will seek new and accurate intelligence that will enable friendly forces to take effective action faster than the adversary). The J-2 must assess the characteristics of the adversary's decision-making process and identify weaknesses that may be exploited. The J-2 must ensure this critical intelligence is appropriately disseminated in a timely manner to the JFC, staff, and components.

b. **Identify, Define, and Nominate Objectives.** All aspects of military planning are dependent on the determination of clearly defined, achievable, and measurable objectives. In the process of identifying and nominating objectives, the J-2 should understand the command's responsibilities; the JFC's mission and intent; means available, including host nation and multinational forces, interagency partners, nongovernmental organizations (NGOs), and intergovernmental organizations (IGOs); the adversary; weather; and characteristics of the operational area. Intelligence should provide the commander with an understanding of the adversary's probable intention, objectives, strengths, weaknesses, critical vulnerabilities, human factors, and COAs to include most dangerous COA and most likely COA. The J-2 also recommends objectives based on adversary critical capabilities, requirements, and vulnerabilities;

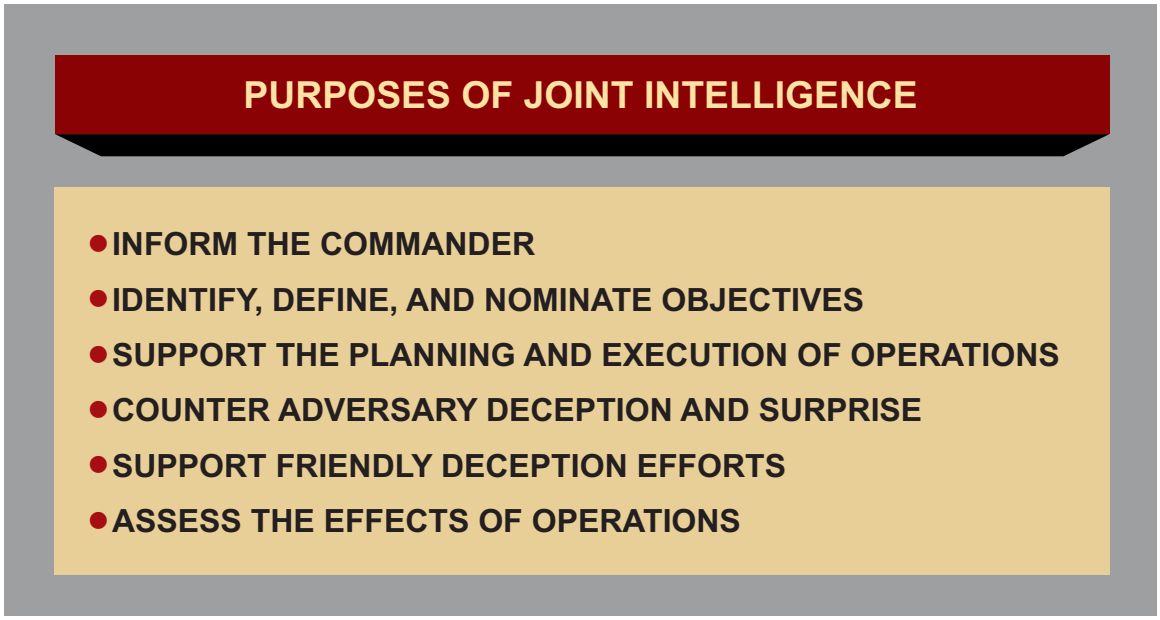


Figure I-2. Purposes of Joint Intelligence

centers of gravity (COGs); and likely COAs. Once these objectives are approved by the commander, the J-2 must continuously review them with respect to the adversary and the changing situation to determine whether they remain relevant to the commander's intent.

c. **Support the Planning and Execution of Operations.** Commanders and staffs at all levels of command require intelligence for planning, directing, conducting, and assessing operations once the objectives, nature, and scope of military operations have been determined by the JFC. This intelligence is crucial to commanders, staffs, and components in identifying and selecting specific objectives and targets with desired and undesired effects, and in determining the means, operations, and tactics to be used in achieving the JFC's overall mission. The J-2 then supports the execution of the plan with the strategic, operational, and tactical intelligence needed to sustain the operation, attain joint force objectives, and support force protection.

d. **Counter Adversary Deception and Surprise.** The method by which J-2s and the intelligence staffs of supporting organizations approach collection, analysis, and dissemination will, to a large extent, determine friendly force vulnerability to adversary deception efforts. Despite the apparent weight of evidence and decision-making predisposition, intelligence analysts must remain sensitive to the possibility that they are being deceived and should consider all possible adversary capabilities and intentions. Similarly, analytical approaches that emphasize anomalies characterized by a lack of activity (e.g., absence of seasonal training, important persons missing from ceremonial events) are particularly valuable. To counter adversary deception efforts, intelligence analysts must confirm their analysis using multiple collection sources and proven analytical methods and processes (e.g., use of red teams, devil's advocates, alternative hypotheses).

e. **Support Friendly Deception Efforts.** Attacking the mind of the adversary – to mislead, delude, or create uncertainty – helps to achieve security and surprise. Intelligence supports effective friendly information operations, especially military deception, through human factors analysis of the adversary leadership, assessing their beliefs, information environment, and decision-making processes. The J-2 also conducts assessments to determine how the adversary is reacting to the friendly deception effort. The process of identifying deception objectives to complement operational objectives should be an interactive process, with the commander in a central role orchestrating the efforts of operations and intelligence resources.

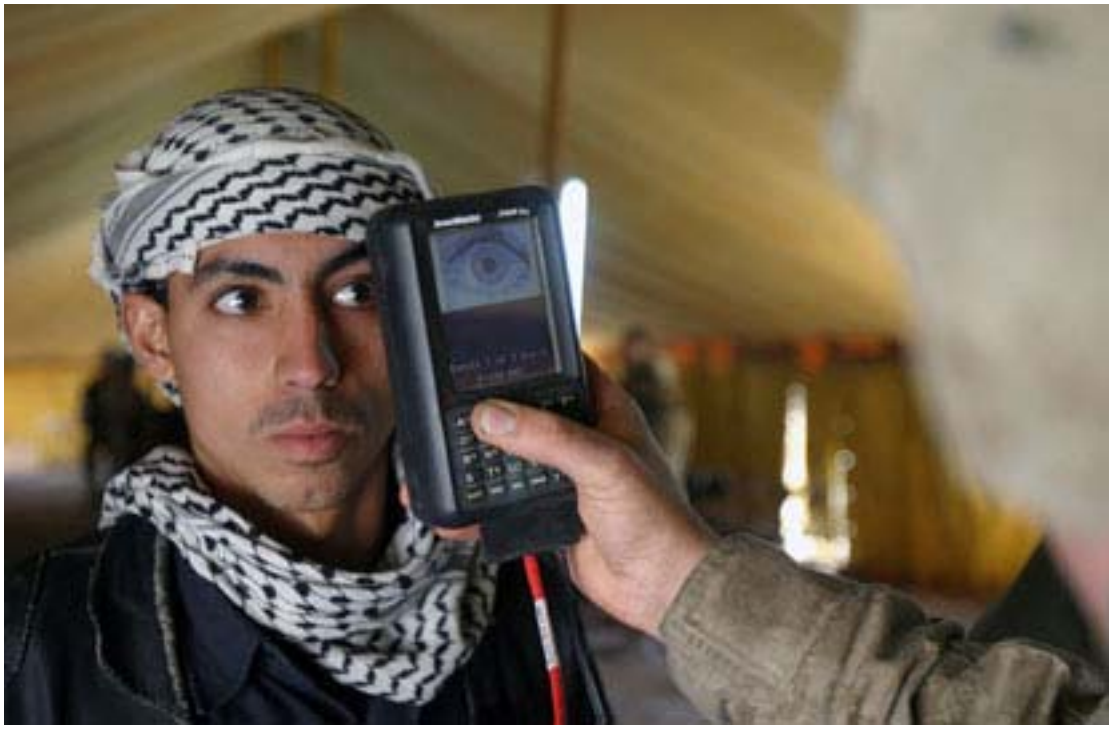
f. **Assess the Effects of Operations.** Intelligence helps evaluate military operations by assessing their impact on the adversary and other relevant aspects of the operational environment with respect to the JFC's intent and objectives. Intelligence should assist JFCs in determining if operations are producing desired or undesired effects, when objectives have been attained, and when unforeseen opportunities can be exploited or require a change in planned operations to respond to adversary (enemy) actions.

"Without [intelligence] you would have only your fears on which to plan your defense arrangements and your whole military establishment. Now if you're going to use nothing but fear and that's all you have, you're going to make us an armed camp. So this kind of knowledge is vital to us."

President Dwight D. Eisenhower
1954

3. Intelligence Disciplines

Intelligence disciplines are well-defined areas of intelligence planning, collection, processing, exploitation, analysis and production, and dissemination using a specific category of technical or human resources. The intelligence disciplines are sometimes further broken down into more specific subcategories as indicated in Figure I-3. Intelligence sources are the means or systems that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. Intelligence sources can be people, documents, equipment, or technical sensors, and are grouped according to one of the seven major intelligence disciplines: geospatial intelligence (GEOINT); human intelligence (HUMINT); signals intelligence (SIGINT); measurement and signature intelligence (MASINT); open-source intelligence (OSINT); technical intelligence (TECHINT); and counterintelligence (CI). These disciplines should be used in concert to complement and support analytic conclusions in an integrated, multidiscipline approach to intelligence analysis.



The Biometric Analysis Tracking System uses thumbprints and facial and retinal scans to identify foreign persons of interest to human intelligence and counterintelligence personnel.

Figure I-3. Intelligence Disciplines, Subcategories, and Sources

The major intelligence disciplines and their subcategories, sources, and capabilities are described in greater detail in Appendix B, "Intelligence Disciplines."

4. The Joint Intelligence Process

The joint intelligence process provides the basis for common intelligence terminology and procedures, and consists of six interrelated categories of intelligence operations. Intelligence operations are wide-ranging activities conducted by intelligence staffs and organizations for the purpose of providing commanders and national-level decision makers with relevant, accurate, and timely intelligence. The six categories of intelligence operations are: planning and direction; collection; processing and exploitation; analysis and

production; dissemination and integration; and evaluation and feedback. In many situations, the various intelligence operations occur nearly simultaneous with one another or may be bypassed altogether. For example, a request for imagery will require planning and direction activity but may not involve new collection, processing, or exploitation. In this example, the imagery request could go directly to a production facility where previously collected and exploited imagery is reviewed to determine if it will satisfy the request. Likewise, during processing and exploitation, relevant information may be disseminated directly to the user without first undergoing detailed all-source analysis and intelligence production. Significant unanalyzed combat information must be simultaneously available to both the commander (for time-critical decision-making) and to the intelligence analyst (for production of current intelligence assessments). Additionally, the activities within each type of intelligence operation are conducted continuously and in conjunction with activities in each of the other categories of intelligence operations. For example, intelligence planning is updated based on previous information requirements being satisfied during collection and upon new requirements being identified during analysis and production. The joint force's mission provides the focal point around which the intelligence process is organized. A simplified conceptual model of the intelligence process is depicted in Figure I-4.

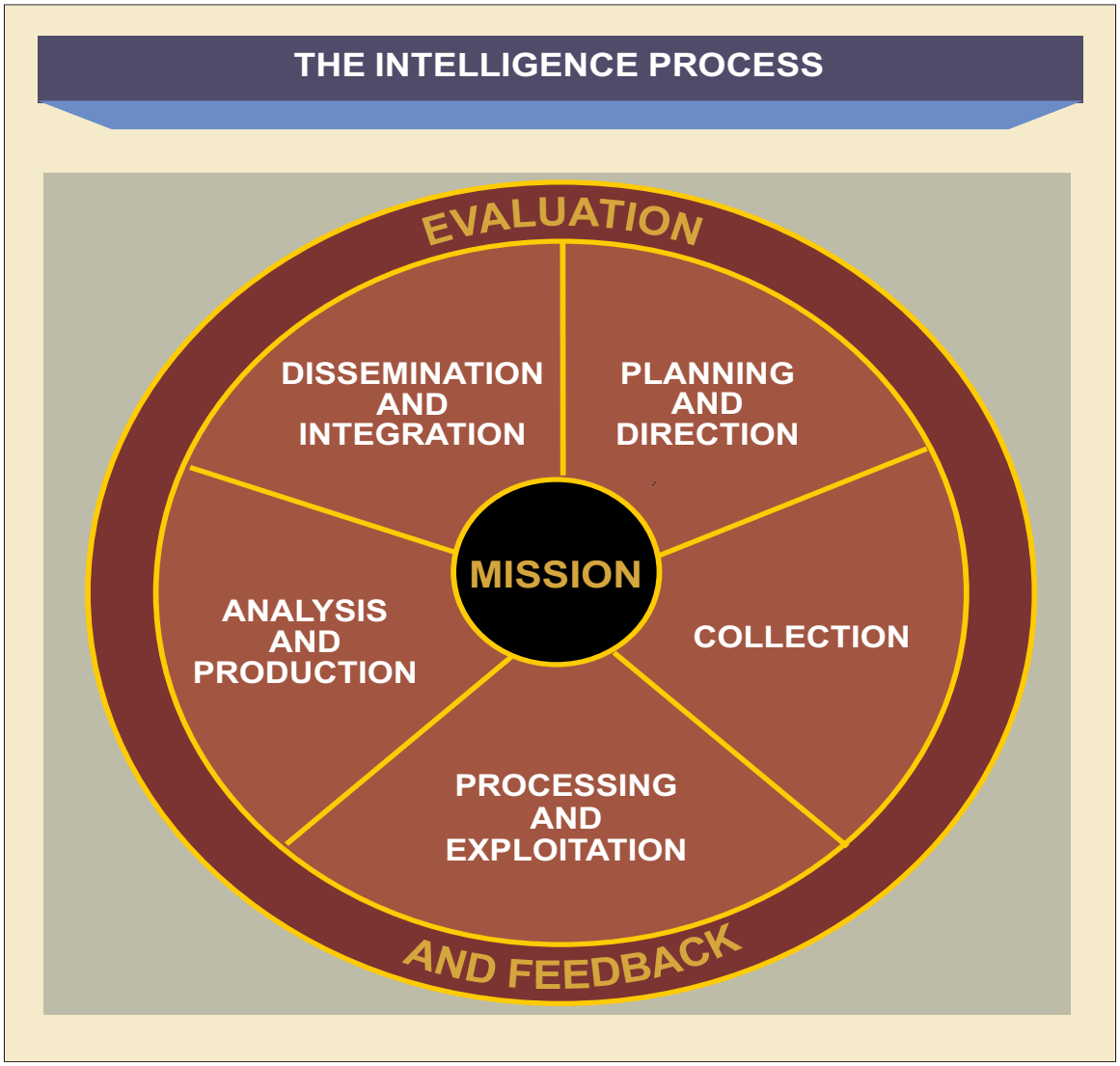


Figure I-4. The Intelligence Process

The joint intelligence process is described as tasks in Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3400.04D, Universal Joint Task List*, which provides a common language and reference system to communicate mission requirements.*

a. **Planning and Direction**. Intelligence planning for rapid response to possible crises occurs well ahead of time as part of a command's overall joint operation planning process. The most likely threat scenarios are used as the core of this planning effort, which includes determining the personnel, equipment, and intelligence architecture essential for generic support to force deployments. When a particular crisis situation unfolds, planners develop an operation order (OPORD). Intelligence input to the OPORD includes an adjusted and updated threat scenario and an intelligence annex that tailors intelligence support to the geographical area, nature of the threat, scope of operations, and assigned forces. Feedback from intelligence personnel to operation planners helps ensure that benefits of lessons learned are incorporated as soon as possible into planning for subsequent operations.

Intelligence support to joint operation planning is discussed in greater detail in Chapter IV, "Intelligence Support to Planning, Executing, and Assessing Joint Operations", Section A.

(1) **Intelligence Requirement and Information Requirement Planning.** During mission analysis, the joint force staff identifies significant gaps in what is known about the adversary and other relevant aspects of the operational environment and formulates intelligence requirements (general or specific subjects upon which there is a need for the collection of information or the production of intelligence). All staff sections may recommend intelligence requirements for designation as priority intelligence requirements (PIRs) – a priority for intelligence support that the commander and staff need. However, the J-2 has overall staff responsibility for consolidating PIR nominations and for making an overall staff recommendation to the commander regarding their approval. Ultimately, the JFC designates PIRs, which together with friendly force information requirements constitute the commander's critical information requirements (CCIRs). Based on identified intelligence requirements (to include PIRs), the intelligence staff develops more specific questions known as information requirements (those items of information that must be collected and processed to develop the intelligence required by the commander). A subset of information requirements that are related to and would answer a PIR are known as essential elements of information (EEIs). Figure I-5 illustrates how information requirements (including EEIs) are formulated from, and are intended to answer, intelligence requirements (including PIRs).

(a) The JFC's total number of PIRs for any phase of an operation should reflect a reasonable balance between mission critical requirements and a finite intelligence support capability. Excessive PIRs may result in unfocused intelligence collection and production. The JFC will develop PIRs that support critical decisions over the course of an operation. By using the PIR as a tool to gather intelligence that is key to critical decisions, the JFC focuses the intelligence system and avoids being overwhelmed with information of peripheral interest. For complex phased operations, separate PIRs should be identified for each phase. As an operation develops, the commander should update PIRs to address new requirements or concerns. Changes in the situation will rule out some PIRs and/or demand the development of new ones as operations progress. PIRs should be ranked and disseminated in priority of importance. The methodology

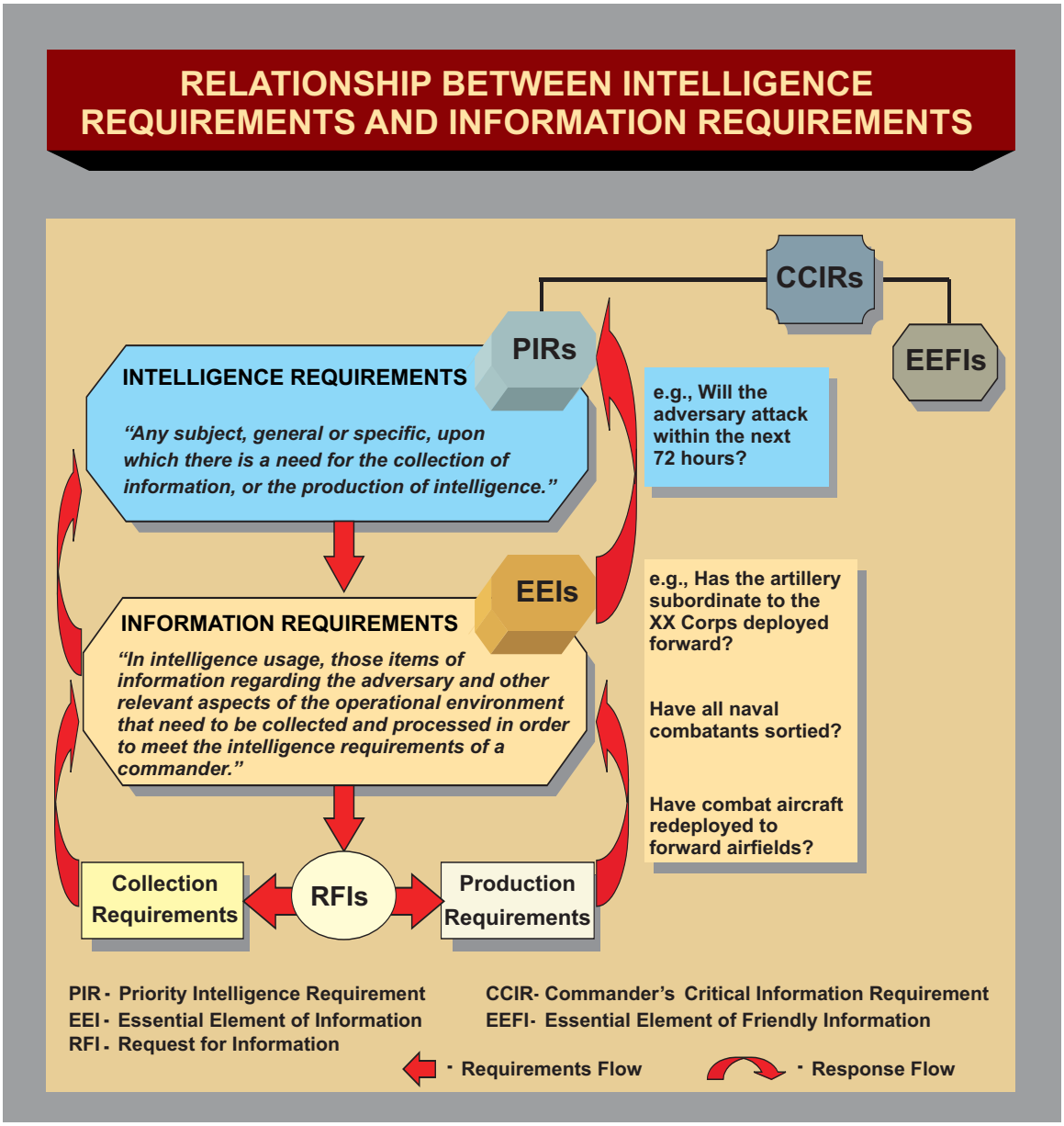


Figure I-5. Relationship Between Intelligence Requirements and Information Requirements

used to build PIRs focuses on the level of operations to be conducted, mission, time frame of expected operations, and priority of requirements.

(b) Using PIRs as the basis, the intelligence staff develops the command's EEIs (the most critical information requirements regarding the adversary and the operational environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision). For example, if the PIR is "Will the enemy attack within the next 72 hours?", the EEIs will be questions such as "Where is the XX Armored Division?"; "Has the artillery subordinate to the XX Corps deployed forward?"; "Are aircraft being loaded with air-to-ground munitions at the forward airfields?"; and "Where are the major surface combatants?" Information requirements (to include EEIs) are concerned with identifying the specific indicators that could fill a gap in the command's

knowledge and understanding of adversary activities and other relevant aspects of the operational environment.

(c) In addition to focusing on the joint force's intelligence requirements, the intelligence staff must be aware of the intelligence requirements of higher, adjacent, subordinate and supporting elements. Subordinate units will expand on the joint force's intelligence requirements by making them specific enough to support their portion of the overall campaign. Conversely, the JFC's PIRs should encompass and prioritize the most urgent intelligence requirements of subordinate, adjacent, and supporting elements. Subordinate force intelligence requirements are addressed and prioritized during planning. Conflicts for resources must be resolved and unnecessary redundancies eliminated.

(d) Once intelligence requirements and information requirements are established, intelligence personnel review existing intelligence databases for answers to the requirements. If the intelligence does not already exist, they issue requests for information (RFIs) and initiate the development or revision of a collection plan. An RFI is a specific time-sensitive ad hoc requirement for information or intelligence products, and is distinct from standing requirements or scheduled intelligence production. An RFI can be initiated at any level of command, and will be validated in accordance with the combatant command's procedures. An RFI will lead to either a production requirement if the request can be answered with information on hand or a collection requirement if the request demands collection of new information. Collection planning and requirement management are major activities during planning and direction.

(e) The most immediate, direct application of PIRs is to assist the J-2 in determining the type and level of intelligence resources required to support the joint force. Intelligence staffs use PIRs as a basis for: formulating statements of intelligence interest to the intelligence community (IC); justifying tasking of national collection resources through the Defense Intelligence Agency (DIA); justifying requests for forces (RFFs) for intelligence, surveillance, and reconnaissance (ISR) resources.

(f) PIRs, EEIs, RFIs, and RFFs should be identified for each phase of an operation and will provide the basis for synchronizing the arrival/availability of required ISR resources by phase. This information will ensure that commanders' specific objectives are reflected in ISR collection plans and national intelligence support plans.

(2) **Collection Planning**. Collection planning matches intelligence collection requirements with appropriate collection capabilities. Collection requirements management (CRM) synchronizes the timing of collection with the operational scheme of maneuver and with other intelligence operations such as processing and exploitation, analysis and production, and dissemination. Intelligence analysts drive this process and provide the collection manager with sufficiently detailed information requirements to allow the formulation of collection requirements and the allocation and apportionment of requirements to collection assets. CRM ensures that all collection requirements are appropriately documented, prioritized, and linked to the commander's decision points, key nodes, and PIRs/EEIs. CRM culminates in preparation and/or revision of the command's intelligence collection plan, which tasks or submits intelligence requirements to the appropriate internal and external supporting intelligence organizations and agencies.

(a) Collection managers continuously monitor the results not only of intelligence collection, but also processing and exploitation, analysis and production, and dissemination to determine if PIRs/EEIs and other information requirements are being satisfied. The effectiveness of the collection plan in meeting the JFC's requirements is continuously assessed by the command's collection managers.

(b) At each level of command, J-2s and senior intelligence officers must know not only their command's intelligence and information requirements, but also be aware of the PIRs of the next higher, adjacent, and supporting and subordinate commands, as well as national-level intelligence requirements. The J-2 collection manager must be knowledgeable about the abilities, limitations, survivability, and required lead times of available collection systems as well as the processing and exploitation, and analysis and production, timelines required to complete a required product. Joint force collection managers must be able to task, or coordinate with, any collection capability assigned to the force and be able to obtain the aid of external resources (e.g., theater and national) in acquiring needed intelligence.

(c) To minimize the effects of enemy deception, and provide the JFC the most accurate intelligence possible, a variety of collection sources are required so that information from one source can be tested or confirmed by others. Multiple collection sources enable collection managers to "cross-cue" between different sources (e.g., using SIGINT direction finding to focus collection by GEOINT systems). Collection systems also need redundancy so that the loss or failure of one collection capability can be compensated for by alternate capabilities. However, careful consideration must be given to having multiple collection sources performing redundant collection, as collection requirements will usually exceed collection systems/missions available.

(d) During collection planning, the intelligence staff coordinates closely with the operations staff. Collection managers, targeteers, and intelligence analysts must work closely together to anticipate operational support requirements and develop and execute adaptive collection plans. Accordingly, the joint force may establish a joint collection management board (JCMB) to monitor and update collection requirements and asset status, and synchronize the collection plan. Active involvement of targeteers, analysts, and operations directorate of a joint staff (J-3) personnel in concert with the collection managers is critical to the success of the JCMB. Collection managers must ensure that the collection plan is synchronized with the operation plan (OPLAN) so that collection efforts are focused correctly at the critical times. Additionally, reconnaissance and surveillance operations must be integrated with other forms of intelligence collection operations and coordinated with CI activities.

(e) There are numerous legal issues associated with intelligence collection on US persons. Commanders and their intelligence staffs must be fully cognizant of their intelligence oversight responsibilities as delineated in Department of Defense (DOD) 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons*. Intelligence collection activities should be coordinated with the servicing staff judge advocate to ensure compliance with the law and any existing rules of engagement.

(3) **Other Planning.** Planning also entails determining intelligence organizational and equipment requirements and creating the necessary intelligence architecture. How the joint task force (JTF) J-2

will be organized and where it will be established are decisions that must be made early in the planning process. Furthermore, the JTF J-2 should, at the earliest possible time, work with the component intelligence elements to minimize confusion and duplication of effort by coordinating their respective roles and responsibilities with regard to analysis, production, and resources.

The unique planning requirements for multinational operations are addressed in Chapter V, "Joint, Interagency, and Multinational Intelligence Sharing and Cooperation."

(a) **Joint intelligence architecture planning** requires early identification and integration of operational architectures (which encompass relevant doctrinal, organizational, and manning considerations) and systems architectures to ensure alignment with and support to the joint force mission. Establishing information flow, timeliness, content, format, and priorities will help shape the requisite joint intelligence architecture's technical specifications to efficiently support a JFC. Joint intelligence architecture planning must ensure survivability, protection (or assurance), and interoperability of both information architectures and the information contained therein for all combinations of government/commercial configurations.

(b) **Anticipated intelligence database access and production requirements** must be coordinated from tactical through national levels. These activities should be directed and coordinated by the joint force J-2 to be collaborative, mutually supporting, and non-duplicative.

(c) **Intelligence dissemination requirements and procedures** must be identified and coordinated with subordinate, adjacent, supporting, and higher intelligence organizations and commands, and with the communications system directorate of a joint staff (J-6). An important consideration is the management of information transmitted over communications paths. JFCs must consider intelligence requirements when prioritizing information dissemination in terms of the product, the available communications paths, and the time sensitivity of the product. Dissemination priorities must be updated throughout the course of the operation.

(d) **Coordination with CI activities** must be accomplished prior to the initiation of operations. Identification of ongoing and planned intelligence activities and JFC intentions will enable CI specialists to assess physical and personnel vulnerabilities and hostile forces' capability to target military operations using technical means, terrorism, espionage, and sabotage, or to evoke agitational interference (e.g., demonstrations, strikes). CI activities may also provide formal liaison with host nation, intelligence, law enforcement, and security activities to assist operations and provide support to the joint force's protection. The joint force J-2 normally organizes a CI section within the J-2 CI/HUMINT staff element (J-2X) to specifically coordinate and deconflict all CI activities: tactical, operational, strategic, and multinational.

Joint Publication (JP) 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations*, provides additional details of the organization and functions of a J-2X staff section within the J-2.*

(e) **Target development** and intelligence planning are interrelated. The intelligence staff of the JFC designated as a supported commander will lead the target intelligence planning effort. The intelligence staff develops supporting guidance in a targeting guidance message that delineates responsibilities for each phase of the joint targeting cycle. Based on the commander's objectives, and desired and undesired effects, targeteers begin a process of target development using intelligence produced by analysts (e.g., target system analysis). As objects or entities are identified, they are added to either the joint target list (JTL), the restricted target list (RTL), or no-strike list (NSL). The JTL contains targets which have military value and do not have any employment restrictions placed on them. The RTL contains targets which have military value, but because of operational phasing or other sensitivities, have had either a timing or employment restriction placed on them. The NSL contains a list of objects or entities which are protected by the law of armed conflict, theater rules of engagement, national policy or other considerations and, so long as they remain on the NSL, may not be struck. Additionally, "no-fire" areas may be designated to protect friendly operations or protect other sensitive targets. As targeteers develop these lists, they coordinate closely with all-source analysts and collection managers to gather additional information, imagery and finished intelligence to provide a more complete picture of the enemy target systems and fill intelligence gaps.

For further information on targeting, target development, and target lists, see JP 3-60, Joint Targeting *and JP 3-09,* Joint Fire Support.

(f) **Geospatial requirements** must be identified early in the planning phase. The geospatial information and services (GI&S) officer on the joint staff works closely with the J-3 and other staff elements to determine requirements and priorities. Maps, charts, digitized products, and precise geodetic coordinates, and other supporting graphics and detailed textual annotations are foundational requirements for collaborative mission planning and execution.

JP 2-03, Geospatial Intelligence Support to Joint Operations*, provides detailed information on obtaining National Geospatial-Intelligence Agency (NGA) support.*

(g) **Administrative planning** is also required. Functions of administrative support that should be addressed as part of the intelligence planning and direction effort include: financial, contracting, training, and personnel support; automated data processing requirements; physical, information and personnel security matters; intelligence and CI oversight compliance; inspector general issues; releasability and disclosure policy; and Freedom of Information Act guidance.

(h) Planning also requires **the early identification of joint force individual intelligence personnel augmentation requirements**, documenting requirements on a joint manning document (JMD), and submitting the JMD through the supporting manpower and personnel directorate of a joint staff to the combatant commander (CCDR) for validation. Likewise, logistic requirements should be identified as early as possible to the joint force's logistics directorate, lift and transportation requirements in the time-phased force and deployment data to the J-3, and communications requirements for intelligence operations to the J-6.

Additional guidance is provided in JP 1-0, Personnel Support to Joint Operations.

The Distributed Common Ground System is a family of fixed and deployable multisource processing systems that facilitate cross-cueing among a wide range of intelligence, surveillance, and reconnaissance sensors.

b. **Collection**. Collection includes those activities related to the acquisition of data required to satisfy the requirements specified in the collection plan. Collection operations management (COM) involves the direction, scheduling, and control of specific collection platforms, sensors, and HUMINT sources and alignment of processing, exploitation, and reporting resources with planned collection. COM duties include development and coordination of sensor employment guidance that helps shape collection plans and strategies and ensures the best allocation of intelligence requirements to collection resources. Collection activities must be revised as required, and include monitoring the overall satisfaction of these requirements and assessing the effectiveness of the collection strategy to satisfy the original and evolving intelligence needs. Collected data is distributed via appropriately classified media/circuits to processing and exploitation elements.

Collection management is addressed in detail in JP 2-01, Joint and National Intelligence Support to Military Operations. *It explains the relationship between CRM and COM. It also details the flow of RFIs from the component or JTF requester to national-level organizations, and the response back to the requester.*

c. **Processing and Exploitation**. During processing and exploitation, raw collected data is converted into forms that can be readily used by commanders, decision makers at all levels, intelligence analysts and other consumers. Processing and exploitation includes first phase imagery exploitation, data conversion and correlation, document translation, and signal decryption, as well as reporting the results of these actions to analysis and production elements. Processing and exploitation may be performed by the same element that collected the data.

(1) An example of processing and exploitation occurs when the technical parameters (frequency, pulse repetition frequency, and bandwidth) detected by an electronic intelligence (ELINT) collection system are compared and associated with the known parameters of a particular radar system. Rather than having to deal with raw ELINT data, the analyst is provided with the essential fact — the identity of the radar.

(2) Different types of data require different degrees of processing before they can be intelligible to the recipient. For example, in the area of SIGINT, processing and exploitation are increasingly automated and are being performed by the collection systems. Captured enemy documents may only require translating before they can be used by analysts. On the other hand, the technical exploitation of an item of enemy equipment may require months of intensive effort before its full capabilities can be determined.

d. **Analysis and Production.** During analysis and production, intelligence is produced from the information gathered by the collection capabilities assigned or attached to the joint force and from the refinement and compilation of intelligence received from subordinate units and external organizations. All available processed information is integrated, evaluated, analyzed, and interpreted to create products that will satisfy the commander's PIRs or RFIs. Intelligence products can be presented in many forms. They may be oral presentations, hard copy publications, or electronic media. Intelligence production for joint operations is accomplished by units and organizations at every echelon. Whereas collection, processing, and exploitation are primarily performed by specialists from one of the major intelligence disciplines, analysis and production is done primarily by all-source analysts that fuse together information from all intelligence disciplines. The product resulting from this multidiscipline fusion effort is known as all-source intelligence.

(1) All-source intelligence production is facilitated through a collaborative, or federated, effort in which information is rapidly and fully shared among geographically dispersed organizations. This approach involves dividing the analysis and production effort among US and partner nation intelligence facilities and organizations worldwide to meet the intelligence needs of the joint force. The intelligence staff should identify the need to federate production with outside commands and agencies as early as possible. In many situations, the level of production, uniqueness of the product, or availability of personnel may require excessive lead time.

(2) **The Defense Intelligence Analysis Program (DIAP) establishes policy, procedures, and responsibilities for intelligence analysis and production**. The DIAP recognizes the vast complexity of achieving comprehensive knowledge of the entire world and therefore divides the analytic effort according to prioritized categories of defense topics, transnational issues, and countries. The DIAP seeks to:

(a) Maintain global situational awareness while gaining a greater depth of knowledge on a limited number of countries and enduring transnational issues that represent the greatest challenge to US national interests.

(b) Maximize resources by assigning clearly defined all-source analytical responsibilities to each combatant command, Service, and DIA.

(c) Assign analytic responsibilities based on capabilities, workforce characteristics and combatant command, Service or DIA's mission requirements.

(d) Bring stability to the all-source analytical workforce through careful assignment of analytical responsibilities and by managing capabilities to ensure a surge capability is maintained within the defense intelligence community.

(e) Support the intelligence priorities established in national policy and strategic guidance (i.e., National Security Presidential Directive – 26, *National Intelligence Priorities Framework*).

(3) A key tool for conducting intelligence analysis and production is the **joint intelligence preparation of the operational environment (JIPOE)** process.

(a) **JIPOE is a systematic approach used by intelligence personnel** to analyze the adversary and other relevant aspects of the operational environment. The JIPOE process is used to define the operational environment, describe the impact of the operational environment on adversary and friendly COAs, evaluate the capabilities of adversary forces operating in the operational environment, and determine and describe potential adversary COAs and civilian activities that might impact military operations. (See Figure I-6)

(b) **Analysts use the JIPOE process** to analyze, correlate, and fuse information pertaining to all relevant aspects of the operational environment (e.g., military, economic, political, social, information and infrastructure systems). The process is also used to analyze adversary capabilities, identify potential adversary COAs, and assess the most likely and most dangerous adversary COAs. The process can be applied to the full range of joint military operations (to include civil considerations) and to each level of war.

The JIPOE process is described in detail in JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

(4) **Intelligence products are generally placed in one of seven production categories:** indications and warning (I&W), current, general military, target, scientific and technical, CI, and estimative intelligence (See Figure I-7). The categories are distinguished from each other primarily by the purpose for which the intelligence was produced. The categories can and do overlap, and the same intelligence and information can be used in each of the categories.

(a) **Indications and Warning.** I&W intelligence concerns foreign developments that could involve a threat to the United States, US or allied military forces, US political or economic interests, or to US citizens abroad. I&W is very time-sensitive. It includes forewarning of adversary actions or intentions; the imminence of nuclear or nonnuclear attack on the United

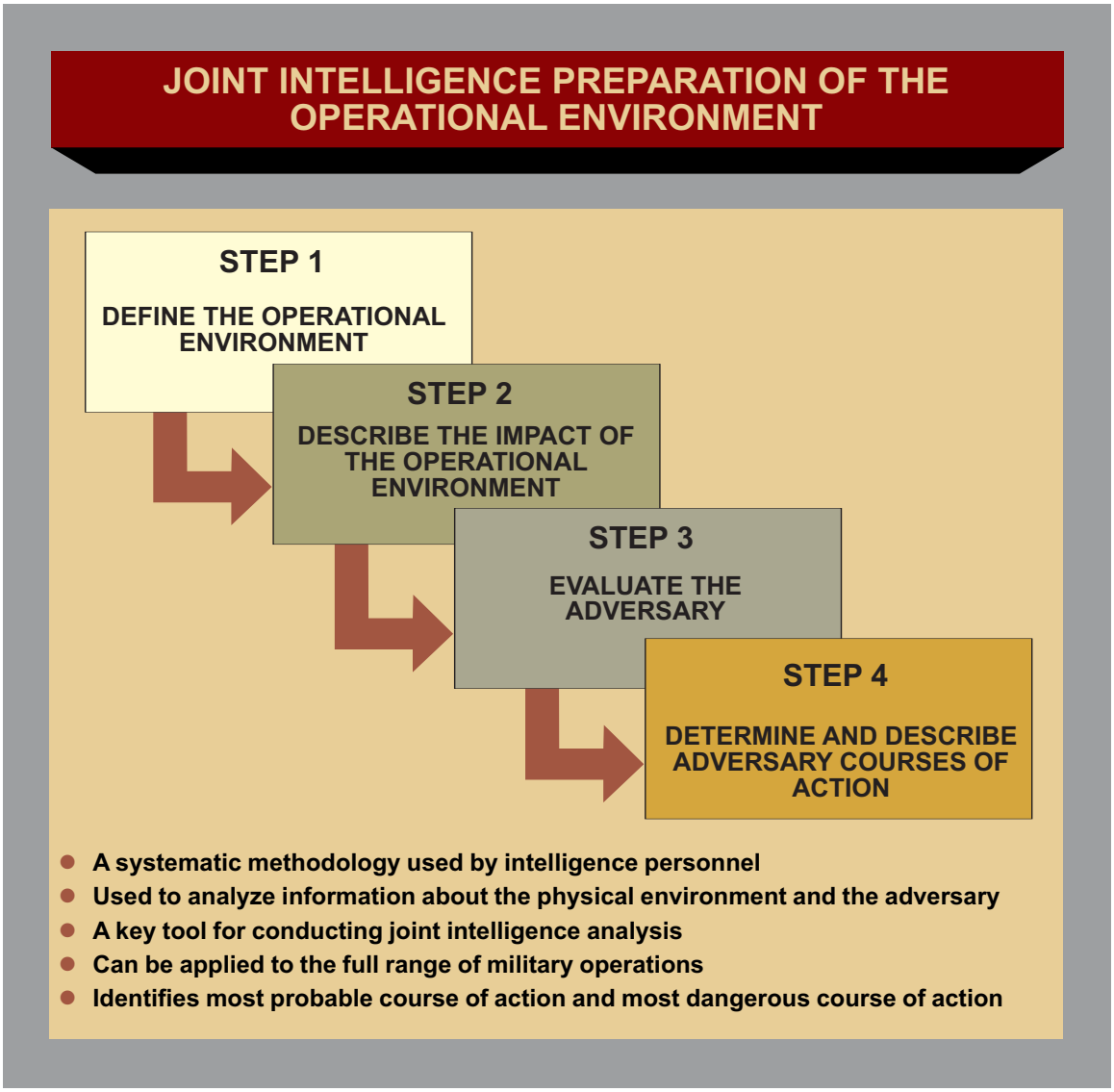


Figure I-6. Joint Intelligence Preparation of the Operational Environment

States, its overseas forces, or allied nations; hostile reactions to US activities; terrorist attacks; and other similar events.

(b) **Current Intelligence.** Current intelligence provides updated support for ongoing operations across the full range of military operations. It involves the integration of time-sensitive, all-source intelligence and information into concise, objective reporting on the current situation in a particular area.

(c) **General Military Intelligence (GMI).** GMI focuses on the military capabilities of foreign countries and organizations and other topics that could affect potential US or multinational military operations. This broad category of intelligence is normally associated with long-term planning. Identifying and monitoring trends affecting national security facilitates the effective application of finite resources to shape the global environment to US advantage.

Figure I-7. Categories of Intelligence Products

However GMI is also an essential tool for the JFC, and should be in place long before the start of preparations for a particular military operation. An up-to-date, comprehensive GMI database is critical to effective, rapid crisis response in an increasingly multipolar, global environment. GMI supports the requirement to quickly respond to differing crisis situations with corresponding intelligence spanning the globe. GMI consists of numerous subcategories. For example, medical intelligence (MEDINT) provides analyses of health threats and foreign medical capabilities, and helps identify mitigation and response options to minimize the impact of health threats. Another important subcategory of GMI is human factors analysis, which provides assessments of the psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups at any level in any state or organization.

See JP 2-01, Joint and National Intelligence Support to Military Operations *and JP 4-02,* Health Service Support *for further information on MEDINT. See JP 2-01.3,* Joint Intelligence Preparation of the Operational Environment *for a more detailed discussion of human factors analysis.*

(d) **Target Intelligence.** Targeting is the process of selecting and prioritizing targets to satisfy stated objectives and matching the appropriate response to them, considering operational requirements and capabilities. Target intelligence entails the analysis of enemy personnel, units, disposition, facilities, systems, and nodes relative to the mission, objectives, and the capabilities at the JFC's disposal, to identify and nominate specific COGs and high-value targets (HVTs) that, if exploited in a systematic manner, will create the desired effects and support accomplishment of the commander's objectives. Throughout the targeting process, it is imperative for intelligence personnel to ensure that all available IC information is fully considered and appropriately de-conflicted to support proper target nomination, target development, and assessment. Target intelligence includes nominations for the NSL and RTL.

See JP 3-60, Joint Targeting, *for further information.*

(e) **Scientific and Technical (S&T) Intelligence.** S&T intelligence encompasses foreign developments in basic and applied sciences and technologies with warfare potential, particularly enhancements to weapon systems. It includes S&T characteristics, capabilities, vulnerabilities, and limitations of all weapon systems, subsystems, and associated materiel, as well as related research and development. S&T also addresses overall weapon systems and equipment effectiveness.

(f) **Counterintelligence.** CI analyzes the threats posed by foreign intelligence and security services and the intelligence activities of non-state actors such as organized crime, terrorist groups, and drug traffickers. CI analysis incorporates all-source information and the results of CI investigations and operations to support a multidiscipline analysis of the force protection threat.

(g) **Estimative Intelligence.** Estimates provide forecasts on how a situation may develop and the implications for planning and executing military operations. Estimative intelligence goes beyond descriptions of adversary capabilities or reporting of enemy activity. It tries to forecast the unknown based on an analysis of known facts using techniques such as pattern analysis, inference, and statistical probability.

e. **Dissemination and Integration**. During dissemination and integration, intelligence is delivered to and used by the consumer. Dissemination is facilitated by a variety of means. The means must be determined by the needs of the user and the implications and criticality of the intelligence. Briefings, video-teleconferences, telephone calls, facsimile transmissions, electronic messages, web pages, and, of increasing importance, network access to computer databases and direct data transfers are all means of dissemination. The diversity of dissemination paths reinforces the need for communications and computer systems interoperability among joint and multinational forces, component commands, DOD organizations, and the interagency community.

(1) **The Global Command and Control System** facilitates the development of an integrated common operational picture (COP), built on a foundation of geospatial information, that displays the disposition of friendly, neutral, and adversary forces throughout the operational environment. Advanced battle management capabilities that allow US forces to be employed faster and more flexibly than those of potential adversaries are dependent upon development of the COP.

(2) The architecture for intelligence dissemination must facilitate the timely transport of functionally integrated or fused intelligence among geographically dispersed producers and diverse joint, multinational, interagency, and local law enforcement consumers. The dissemination architecture allows intelligence organizations external to the joint force to satisfy joint force intelligence needs to the maximum extent possible if they have sufficient knowledge of the joint force's requirements through preplanned PIRs . Additionally, intelligence organizations should push intelligence to the consumer (using the most expeditious means available), and accommodate the consumer's pull on demand (allowing automated access to theater and national databases). This construct results in timely intelligence, makes maximum use of automation, and minimizes the flow of RFI messages and intelligence reports. Broadcasts such as the integrated broadcast service and the tactical related applications are examples of over-the-air updates that provide time-sensitive intelligence to tactical commanders.

Chapter V, "Joint, Interagency, and Multinational Intelligence Sharing and Cooperation," *provides a more comprehensive discussion of intelligence dissemination architectures and requirements.*

(3) Supporting intelligence organizations must emphasize providing intelligence to the consumer using the best available, and most secure, technology. Intelligence organizations at all levels must ensure precision and commonality in terminology to minimize the possibility of confusion on the part of users reviewing assessments and estimates.

(4) **Intelligence organizations at all levels must ensure that their products are getting to users when they are needed**. Simply putting the product into the dissemination system is not enough. Intelligence organizations must initiate and maintain close contact with users to ensure that the product has been received and meets their requirements. If they fail to do this, all other aspects of the intelligence effort are rendered meaningless.

(5) After intelligence products are delivered, intelligence personnel and organizations are responsible for continuing to support users as they integrate the intelligence into their decision-making and planning processes. Products may require further clarification or they may raise new issues that must be immediately addressed. Products may need to be related to a larger intelligence picture. Products may cause the user to consider new operational concepts that require the intelligence to be interpreted in a new context.

(6) Rather than being the end of a process, the integration of intelligence is a continuous dialogue between the user and the producer. How or even whether intelligence is used is ultimately up to the user. The role of the producer is to ensure that the user has the best intelligence possible for decision-making.

f. **Evaluation and Feedback**. During evaluation and feedback, intelligence personnel at all levels assess how well each of the various types of intelligence operations are being performed. Commanders and operational staff elements must provide feedback. When areas are identified that need improvement, the necessary changes are made. Evaluation and feedback may also serve to refine collection requirements and priorities in phased operations.

(1) **Evaluation and feedback are continuously performed during each category of intelligence operation.** Intelligence planners, collectors, analysts, and disseminators coordinate and cooperate to determine if any of the various intelligence operations require improvements. Individual intelligence operators aggressively seek to improve their own performance and the performance of the activities in which they participate.

(2) An important aspect of evaluation and feedback is identifying and reporting issues or potential lessons that would affect the warfighter. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3150.25B, *Joint Lessons Learned Program (JLLP),* provides basic guidance and direction on establishing internal lessons learned programs and how to enter issues into a resolution process. Combatant commands, Services, and combat support agencies are responsible for providing more specific guidance on how to share observations from joint operations with assigned forces or

personnel. It is essential that intelligence organizations outside the joint force fully participate in the JLLP process to ensure that the benefits of lessons learned are disseminated as widely as possible.

5. Intelligence and the Levels of War

a. **Levels of War**. JP 3-0, *Joint Operations*, discusses three levels of war: strategic, operational, and tactical. The levels provide a doctrinal perspective that clarifies the links between strategic objectives, effects, and tactical actions and assists commanders in visualizing a logical flow of operations, allocating resources, and assigning tasks. Actions can be defined as strategic, operational, or tactical based on their contribution to achieving strategic, operational, or tactical objectives, but many times the accuracy of these labels can only be determined during post-mission analysis or historical studies.

(1) All levels of war have corresponding levels of intelligence operations. The construct of strategic, operational, and tactical levels of intelligence aids JFCs and their J-2s in visualizing the flow of intelligence from one level to the next. This construct facilitates the allocation of required collection, analytical, and dissemination resources and permits the assignment of appropriate intelligence tasks to national, theater, component, and supporting intelligence elements.

(2) Intelligence operations must support commanders at all levels, both horizontally and vertically. Strategic intelligence operations provide continuity and depth of coverage even while the joint force is deploying. During campaign planning, strategic and operational intelligence operations focus on providing to the JFC information required to identify the adversary's COGs, COAs, and HVTs. During execution, operational intelligence operations provide the JFC with relevant, timely, and accurate intelligence relating to the accomplishment of campaign or major operation objectives.

(3) Levels of command, size of units, types of equipment, or types of forces or components are not associated with a particular level of intelligence operations. National assets such as intelligence and communications satellites, usually considered in a strategic context, are an important enabler of tactical operations. Conversely, troops operating in the field can gather intelligence of strategic importance.

(4) Operational and tactical intelligence operations reduce the JFC's uncertainty about the adversary and the operational environment. **Operational and tactical intelligence operations, in conjunction with appropriate assessments, provide the JFC the information required to identify adversary critical vulnerabilities, COGs, and critical nodes for the optimum application of all available resources, thereby allowing the JFC to most effectively employ the JTF's capabilities**. Figure I-8 depicts the levels of intelligence.

b. **Strategic Intelligence**

(1) **National strategic intelligence** is produced for the President, Congress, Secretary of Defense, senior military leaders, and the CCDRs. It is used to develop national strategy and policy, monitor the international situation, prepare military plans, determine major weapon systems and force structure requirements, and conduct strategic operations. Strategic intelligence operations also produce

the intelligence required by CCDRs to prepare strategic estimates, strategies, and plans to accomplish missions assigned by higher authorities.

(2) **Theater strategic intelligence** supports joint operations across the range of military operations and determines the current and future capabilities of adversaries that could affect the national security and US or allied interests. Theater strategic intelligence includes determining when, where, and in what strength the adversary will stage and conduct theater level campaigns and strategic unified operations.

c. **Operational Intelligence**

(1) Operational intelligence is primarily used by CCDRs and subordinate JFCs and their component commanders. Operational intelligence focuses on adversary military capabilities and intentions. Operational intelligence helps the JFC and component commanders keep abreast of events within their area of interest and helps commanders determine when, where, and in what strength the adversary might stage and conduct campaigns and major operations. During counterinsurgency and counterterrorism operations, operational intelligence is increasingly concerned with stability operations and has a greater focus on political, economic, and social factors.

(2) Within the operational area, operational intelligence addresses the full range of military operations, facilitates the accomplishment of theater strategic objectives, and supports the planning and conduct of joint campaigns and subordinate operations. Operational intelligence focuses on providing the JFC information required to identify adversary COGs and provides relevant, timely, and accurate intelligence and assessments. Operational intelligence also includes monitoring terrorist incidents and nature or man-made disasters and catastrophes.

d. **Tactical Intelligence**

(1) Tactical intelligence focuses on combat intelligence, which is used by commanders, planners, and operators for planning and conducting battles, engagements, and special missions. Relevant, accurate, and timely combat intelligence allows tactical units to achieve positional and informational advantage over their adversaries. Precise threat and target status reporting, in particular, is essential for success during actual mission execution. Another critical focus of tactical intelligence is obstacle intelligence — efforts to detect the presence of enemy (and natural) obstacles, determine their types and dimensions, and provide the necessary information to plan appropriate bypass, combined arms breaching, or clearance operations to negate the impact on the friendly scheme of maneuver.

(2) Tactical intelligence addresses the threat across the range of military operations. Tactical intelligence operations identify and assess the adversary's capabilities, intentions, and vulnerabilities, as well as describe the physical environment. Tactical intelligence seeks to identify when, where, and in what strength the adversary will conduct tactical level operations. During counterinsurgency and counterterrorism operations, tactical intelligence is increasingly focused on identifying threats to stability operations. Together with CI, tactical intelligence will provide the commander with information on the imminent threats to the force from terrorists, saboteurs, insurgents, and foreign intelligence collection.

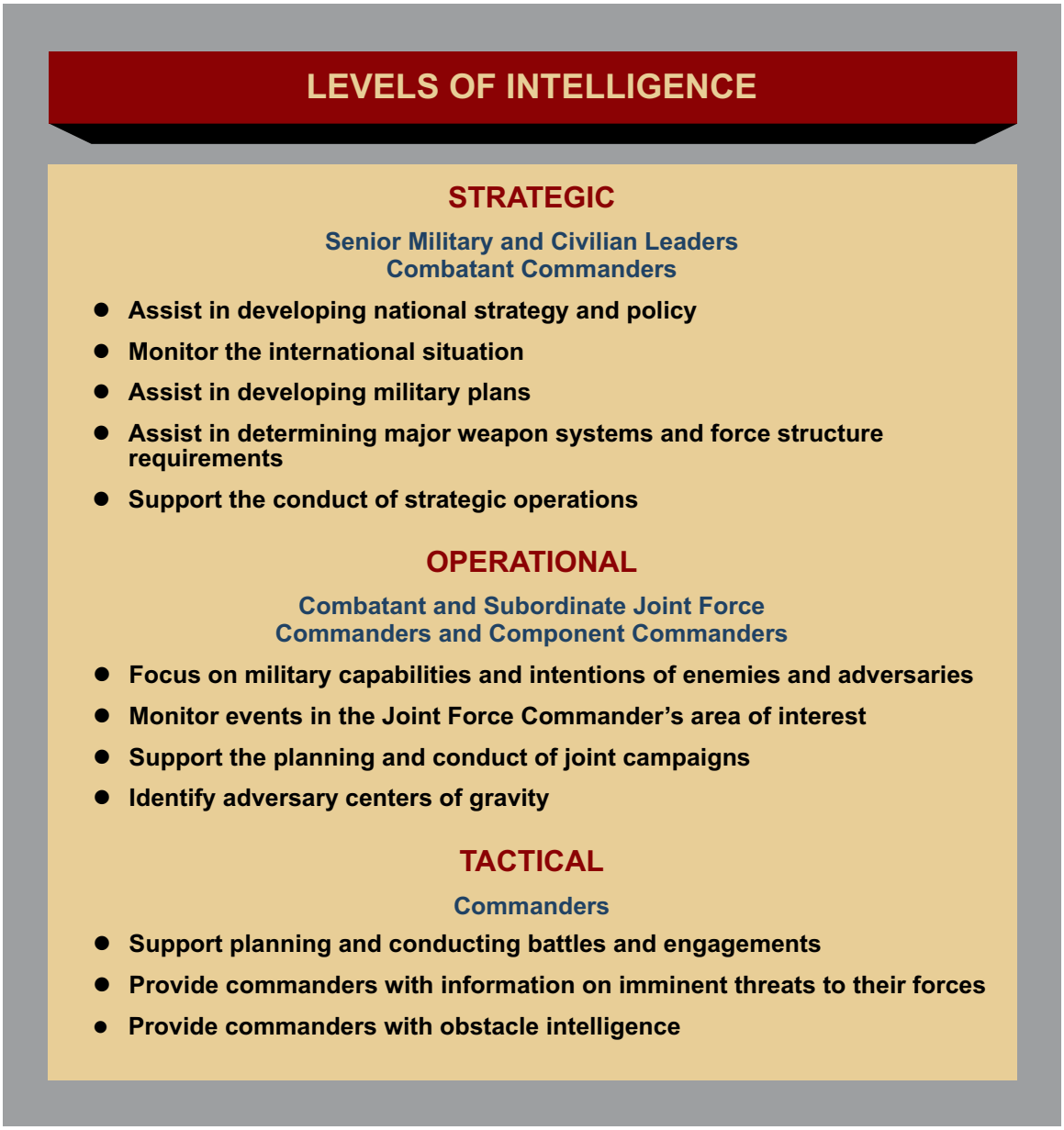


Figure I-8. Levels of Intelligence

6. Intelligence and the Range of Military Operations

JP 3-0, *Joint Operations*, divides the range of military operations into three major categories: military engagement, security cooperation, and deterrence; crisis response and limited contingency operations; and major operations and campaigns. Intelligence operations continue throughout the range of military operations. In fact, peacetime intelligence operations provide the national leadership with the intelligence needed to realize national goals and objectives, while simultaneously providing military leadership with the intelligence needed to accomplish missions and implement the national security strategy. During peacetime, intelligence helps commanders project future adversary capabilities; make acquisition decisions; protect technological advances; define weapons systems and ISR systems requirements; shape organizations; and design training to ready the joint force. Intelligence assets monitor foreign states, volatile regions, and transnational issues to identify threats to US interests in time for senior

military leaders to respond effectively. Intelligence support is equally critical throughout the range of military operations.

a. **Intelligence Support During Military Engagement, Security Cooperation, and Deterrence Operations.** Maintaining a forward presence enables US forces to gain regional familiarity and develop a common understanding of important cultural, historical, interpersonal, and social differences. Activities such as professional military exchanges, forward basing, and cooperative relationships with multinational partners enhance US forces' ability to shape potential military engagement, security cooperation, and deterrence operations, gain an understanding of multinational tactics and procedures, enhance information sharing, and establish mutual support with host country nationals. Intelligence support is essential to activities such as emergency preparedness, arms control verification, combating terrorism, counterdrug operations, enforcement of sanctions and exclusion zones, ensuring freedom of navigation and overflight, nation assistance, protection of shipping, shows of force, and support to insurgency and counterinsurgency operations. Intelligence develops knowledge of the operational environment in relation to the JFC's questions concerning actual and potential threats, terrain, climate and weather, infrastructure, cultural characteristics, medical conditions, population, and leadership. Intelligence helps the JFC determine which forces to employ and assists in estimating the duration of the operation.

b. **Intelligence Support During Crisis Response and Limited Contingency Operations.** Intelligence provides assessments that help the JFC decide which forces to deploy; when, how, and where to deploy them; and how to employ them in a manner that accomplishes the mission. The intelligence requirements in support of crisis response and limited contingency operations such as noncombatant evacuation operations, peace operations, foreign humanitarian assistance, recovery operations, consequence management actions associated with chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE), strikes and raids, homeland defense, and civil support are similar to those required during major operations. During disaster relief operations, intelligence can play an important role in surveying the extent of damage and can assist in planning for the deployment of relief forces. Intelligence is essential to protect joint forces participating in these operations. While intelligence efforts are supporting peacekeeping operations, intelligence must also provide the JFC with I&W of any possible escalation of violence and a firm basis upon which to develop necessary OPLANs. Intelligence professionals providing support for homeland defense and civil support shall comply with intelligence oversight policies and regulations. Intelligence activities carried out as part of civil support operations should be reviewed by competent legal authority.

The Secretary of Defense may use his authorities to permit US Northern Command (USNORTHCOM) to use its intelligence capabilities, and the Joint Intelligence Operations Center - North may task Department of Defense (DOD) intelligence components, to provide support to USNORTHCOM missions other than foreign intelligence or counterintelligence in continental United States (CONUS) special missions. This is only when both the mission and use of those DOD intelligence component assets, platforms and/or personnel is approved by the Secretary of Defense. This authorization should be documented in the request for forces submitted to the Joint Staff and Secretary of Defense for review and approval. The

approval for use of the requested DOD intelligence component capabilities and any operational parameters or limitations on use of the information collected must be specified in the execute order approved by the Secretary of Defense before DOD intelligence component forces can be tasked to accomplish missions in CONUS.

c. **Intelligence Support During Major Operations and Campaigns.** Intelligence identifies enemy capabilities, helps identify the COGs, projects probable COAs, and assists in planning friendly force employment. By determining the symmetries and asymmetries between friendly and enemy forces, intelligence assists the JFC and operational planners in identifying the best means to accomplish the joint force mission. For example, in support of joint information operations (IO), intelligence provides the JFC and component commanders with information on the relevant physical, informational, and cognitive properties of the information environment and its impact on military operations; estimates of what the enemy's information capabilities are; when, where, and how the joint force can exploit its information superiority; and the threat the enemy poses to friendly information and information systems.

(1) Intelligence that enables the JFC to focus and leverage combat power and to determine acceptable risk is key to allowing the JFC to achieve powerful, dynamic concentrations when and where the enemy is vulnerable, and permits the JFC to exploit the maximum range of assigned, attached, or supporting weapon systems. Intelligence provides key elements to successful targeting by providing identification of HVTs, collection to develop these targets, weapons and platform delivery recommendations, collateral damage estimates, and the assessment of the accuracy of delivery means and the extent of damage to, or effect on, the targets. By helping the commander form the most accurate possible vision of future events in the operational environment, intelligence serves to expand the timeline within the decision-making process.

(2) Wartime support to the commander must be anticipatory and precise. Intelligence must maximize and synchronize support to the JFC by focusing on satisfying the command's PIRs. Intelligence provided to the JFC should anticipate operational needs and properly balance the qualities of timeliness, accuracy, usability, completeness, relevancy, objectivity, and availability. The result of the intelligence process must be a product or service to the commander that actively supports and enhances the commander's vision of the operational environment in a readily usable manner.

7. The Role of Intelligence in Military Operations

Intelligence constitutes one of six basic groups of joint functions (related capabilities and activities grouped together to help JFCs integrate, synchronize, and direct joint operations). Other joint functions include command and control, fires, movement and maneuver, protection, and sustainment. Some functions, such as command and control and intelligence, apply to all operations. Others, such as fires, apply as required by the JFC's mission.

a. Intelligence plays a critical and continuous role in supporting military operations. Advances in computer processing, precise global positioning, and telecommunications provide commanders with the

capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and disseminate relevant data to thousands of locations. These capabilities, combined with the ability to deny or degrade the enemy's ability to collect, process, and disseminate an uninterrupted flow of information, provide the JFC with information superiority. Likewise, the fusion of all-source intelligence along with the integration of sensors, platforms, command organizations, and logistic support centers allows a greater number of operational tasks to be accomplished faster, and enhances awareness of the operational environment — a key component of information superiority.

b. The most important role of intelligence in military operations is to assist commanders and their staffs in understanding and visualizing relevant aspects of the operational environment. This includes determining adversary capabilities and will, identifying adversary critical links, key nodes, HVTs and COGs, and discerning adversary probable intentions and likely COAs. Visualization of the operational environment requires a thorough understanding of the characteristics of the operational area and the current dispositions and activities of adversary and neutral forces. It requires knowing the adversary's current and future capability to operate throughout the operational environment based on a detailed analysis of the impact of weather, geography, and other relevant considerations. Most important, visualization requires understanding the adversary's objectives, identifying how the adversary might fulfill those objectives, and determining the adversary's readiness to achieve the objectives. Together, all these factors make a critical contribution to the JFC's capability to achieve information superiority. However, intelligence must also enable the JFC to know the potential and probable future state of events well in advance of the adversary. This knowledge allows the JFC to predict the adversary's future COA and scheme of maneuver, and to anticipate adversary actions and plan detailed countermeasures.

c. The use of "red teams" is critical to the ability of commanders and their staffs to understand the adversary and visualize the relevant aspects of the operational environment. Red teams are organizational elements comprised of trained, educated, and practiced experts that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. Red teams assist joint operation planning by validating assumptions about the adversary, participating in the wargaming of friendly and adversary COAs, and providing a check on the natural tendency of friendly forces to "mirror image" the adversary (i.e., to ascribe to an adversary the same motives, intent, and procedures that guide friendly forces).

d. **Determining the adversary's intention is the most difficult challenge confronting intelligence.** The factor which makes this so difficult is the drawing of conclusions based upon the dynamic process of action and reaction between friendly and enemy forces. Clausewitz referred to this as the "process of interaction." He believed that "the very nature of interaction is bound to make it unpredictable." Estimating the outcome of the "process of interaction" requires the intelligence officer to know what future friendly actions are planned and then to simultaneously forecast the following factors: the likelihood of the friendly action being detected by the adversary; how the adversary will interpret the friendly action; the adversary's future capabilities; and finally, how the adversary will most likely react. The long-term projection of adversary intention is particularly difficult because, at the time that intelligence personnel are being asked to determine it, adversaries may not yet have formed their intention, may be in the process of changing their intention, or may not yet have undertaken any detectable action that

would provide indicators of their future plans. Moreover, an adversary will often use a deception plan to mislead friendly analysts. A properly trained and augmented red team can reduce the risk associated with long term prediction of enemy reaction by offering alternative perspectives based on knowledge of the adversary's culture, doctrine, capabilities, and other relevant factors.

(1) A simple example of the "process of interaction" is the situation in which an intelligence officer, having detected certain adversary actions and correctly determined the adversary's intention, forecasts that the adversary is preparing to attack. The commander reacts by having friendly forces take appropriate defensive measures. The adversary commander, however, detecting these actions and deciding that attacking is no longer a desirable COA, cancels the attack. In this example, adversary actions produced a friendly reaction resulting in changes to the adversary's intention. This situation is known as the **"paradox of warning"** and is depicted in Figure I-9.

(2) Accurate forecasts should inform the JFC of the full range of actions open to the adversary and go on to identify which actions are most likely. The JFC must, however, understand the dynamics that are at play in forecasting future events.

Figure I-9. The Paradox of Warning

Intentionally Blank

CHAPTER II
PRINCIPLES OF JOINT INTELLIGENCE

"Tell me what you know … tell me what you don't know … tell me what you think — always distinguish which is which."

General Colin Powell, USA
Chairman of the Joint
Chiefs of Staff, 1989-1993

1. Introduction

This chapter combines intelligence theory and operating experience into fundamental principles that are intended to contribute to effective and successful joint intelligence operations. The following principles for conducting joint intelligence activities are appropriate at all levels of war across the range of military operations (See Figure II-1).

2. Perspective — (Think Like the Adversary)

Intelligence analysts must seek to understand the adversary's thought process, and should develop and continuously refine their ability to think like the adversary. They must offer this particular expertise for the maximum benefit of the JFC, joint staff elements, and component commands during planning, execution, and assessment. The JFC should require the J-2 to assess all proposed actions from the following perspective: "How will the adversary likely perceive this action, and what are the adversary's probable responses?" A human factors analysis of adversary leaders assists in gaining insights into their probable responses. Carrying out these intelligence responsibilities calls for sound judgment as well as expertise.

Figure II-1. Principles of Joint Intelligence

a. The ability to think like the adversary is predicated on a detailed understanding of the adversary's goals, motivations, objectives, strategy, intentions, capabilities, methods of operation, vulnerabilities, and sense of value and loss. Additionally, the J-2 must understand the culture, religions, sects, ethnicities, social norms, customs and traditions, languages, and history of the adversary as well as neutrals and noncombatants in the operational environment. The ability of intelligence analysts to think and react like the adversary is of particular value during the wargaming of various COAs and the determination of enemy HVTs. Properly trained personnel formed in either structured or ad hoc red teams, can insure the enemy is appropriately portrayed and fought during the war game.

b. Understanding how an adversary will adapt to the environment, conceptualize the situation, consider options, and react to our actions, must be an inextricable part of a continuing interaction of the intelligence staff with the JFC and other staff elements. This comprehensive understanding is essential to: recognizing challenges to our national security interest; establishing security policy; when appropriate, formulating clear, relevant, and attainable military objectives and strategy; determining, planning, and conducting operations that will help attain US policy objectives; and identifying the adversary's strategic and operational COGs.

"Great advantage is drawn from knowledge of your adversary, and when you know the measure of his intelligence and character you can use it to play on his weaknesses."

Frederick the Great,
Instructions for His Generals, 1747

3. Synchronization — (Synchronize Intelligence with Plans and Operations)

Intelligence must be synchronized with operations and plans in order to provide answers to intelligence requirements in time to influence the decision they are intended to support. Intelligence synchronization requires that all intelligence sources and methods be applied in concert with the OPLAN and OPORD. OPLAN and OPORD requirements therefore constitute the principal driving force that dictates the timing and sequencing of intelligence operations. Intelligence planning and direction, collection, processing and exploitation, analysis and production, and dissemination must all be accomplished with sufficient lead time to permit the integration of the intelligence product in operational decision-making and plan execution. Effective synchronization results in the maximum use of every intelligence asset where and when it will make the greatest contribution to success. Coordination among each of the various types and levels of intelligence operations, and the integration of the overall intelligence process with plans and operations comprise intelligence synchronization.

a. The most common error in attempting to synchronize intelligence with operations and plans is the failure to build sufficient lead time for intelligence production and operational decision- making. To avoid "late" intelligence, the JFC, J-3, and the plans directorate of a joint staff (J-5) in collaboration with the J-2, should establish a suspense or specify a timeframe during which each intelligence requirement must be answered in order to support decision-making and operation planning. Likewise, the J-2 must provide sufficient lead time for the collection, processing, analysis, and dissemination of the requisite intelligence to meet the commander's specified deadline. To achieve synchronization, the J-2 must be

involved as early as possible in the operation planning effort and must play an active role during the wargaming and analysis of all COAs and plans.

b. The commander drives the intelligence synchronization effort by determining the friendly COA, PIRs, and points in time and space (decision points) where critical events and activity would necessitate a command decision. Decision points are identified on a decision support template developed during the JIPOE process and wargaming. This template provides the basis for PIR development, optimized collection planning, and the formulation of an intelligence synchronization matrix.

4. Integrity — (Remain Intellectually Honest)

Intellectual integrity must be the hallmark of the intelligence profession. It is the cardinal element in intelligence analysis and reporting, and the foundation on which credibility with the intelligence consumer is built. Integrity requires adherence to facts and truthfulness with which those facts are interpreted and presented. Moral courage is required to remain intellectually honest and to resist the pressure to reach intelligence conclusions that are not supported by facts. The methodology, production, and use of intelligence must not be directed or manipulated to conform to a desired result; institutional position; preconceptions of a situation or an adversary; or predetermined objective, operation, or method of operations. **Intelligence concerning a situation is one of the factors in determining policy, but policy must not determine the intelligence.**

a. Intelligence analysts should take active measures to recognize and avoid cognitive biases which affect their analysis. Cognitive bias results when intelligence analysts see the world through lenses colored by their own perceptions and paradigms. Intelligence is filtered through these paradigms and perceptions, and analysts are tempted to fit information into pre-existing beliefs and discard information that does not fit.

b. Intelligence analysts must continuously guard against becoming rigidly committed to a specific interpretation of a set of facts (i.e., they must not ignore or downplay the significance of facts that do not fit a preferred hypothesis or that contradict a previous assessment). Intelligence must be continuously reviewed and where necessary revised, taking into account all new information and comparing it with what is already known. Intelligence professionals must have the integrity to admit analytic misjudgments and the courage to change or adjust previously stated assessments when warranted by new information. Intelligence analysts must vigilantly avoid group think; a mode of thinking that occurs when group members strive for unanimity and fail to examine alternative hypotheses. **Likewise, intelligence analysts must guard against any temptation to court favor from superiors by blindly following a hypothesis that supports a decision maker's predilections.**

c. The same moral courage and intellectual integrity must extend to reporting what is not known; no matter how unpleasant that may be in the short term. Intelligence professionals must avoid the temptation to make assessments appear more definitive than may be warranted by the facts. Intellectual integrity requires the intelligence professional to distinguish for the commander those conclusions that are

solidly grounded in fact and those that are extrapolations or extensions of the fact. **The commander cannot be left with uncertainty regarding what is fact, what is opinion, and what is unknown.**

INTEGRITY UNDER PRESSURE

At the outset of the Spanish-American War, Colonel Arthur L. Wagner was head of the Military Information Division (the War Department's embryonic intelligence organization). Driven by public sentiment, President McKinley and Secretary of War Russell A. Alger were determined to attack Spanish forces in Cuba not later than summer 1898. Wagner at once prepared a careful assessment of the Spanish forces, terrain, climate and environmental conditions in Cuba – the basic intelligence needed for operational planning. Wagner's assessment also identified recurring outbreaks of yellow fever in Cuba during the summer months as a crucial planning consideration. At a White House meeting, Wagner recommended postponement of any invasion until the winter months in order to reduce what would otherwise be heavy American losses from the disease. President McKinley reluctantly endorsed his view. As they left the meeting, Secretary of War Alger was furious with Colonel Wagner.

"You have made it impossible for my plan of campaign to be carried out," he told Wagner. "I will see to it that you do not receive any promotions in the Army in the future."

The Secretary of War made good on his promise, for although Colonel Wagner was promoted years later to brigadier general, the notice of his appointment reached him on his death bed. Furthermore, Alger influenced McKinley to reauthorize a summer invasion of Cuba. Fortunately United States forces won a quick victory, but as Wagner predicted, the effects of disease soon devastated the force. The ravages of yellow fever, typhoid, malaria and dysentery accounted for more than 85 percent of total casualties and were so severe that by August 1898 less than one quarter of the invasion force remained fit for service.

According to his peers, Wagner deliberately jeopardized his career in order to satisfy a sense of duty, rather than bow to political pressure. Information that American lives could be saved by avoiding the worst time of the year for yellow fever was more important to him than currying favor with the Secretary of War.

SOURCE: Various Sources

5. Unity of Effort — (Cooperate to Achieve a Common End State)

Unity of effort – coordination through cooperation and common interests to achieve a desired end state – is essential to effective joint intelligence operations. Unity of effort is facilitated by

centralized planning and direction and decentralized execution of intelligence operations, which enables JFCs to apply all available ISR assets wisely, efficiently, and effectively. It optimizes intelligence operations by reducing unnecessary redundancy and duplication in intelligence collection and production. Unity of effort requires intelligence operations, functions and systems that are coordinated, synchronized, integrated, and interoperable. All intelligence organizations (joint, national, and multinational) operating in a JFC's operational area must have a clear understanding and common acceptance of the command's desired effects, objectives, and end state.

a. All organic and attached intelligence assets operating in the JFC's operational area and all national and theater intelligence resources supporting the joint force should be integrated in an interoperable and seamless architecture so that all joint force elements have access to required intelligence. This approach allows the JFC and J-2 to orchestrate pertinent intelligence activities to meet the joint force's intelligence requirements. Of particular importance is the seamless provision of joint intelligence support to operational forces across the range of military operations as they deploy from one theater to another. To effectively plan and execute unit missions, deploying intelligence personnel must know the supported theater's concept of intelligence operations, intelligence architecture, estimate of the situation, map standards, and other theater-specific requirements. This information should be rapidly provided to deploying forces in a standardized electronic format by intelligence producers. This focuses the intelligence community's effort on satisfying operational requirements.

b. Achieving unity of effort is most challenging during the coordination of multinational operations or when supporting another lead federal agency. Unity of effort in this type of environment requires establishing an atmosphere of trust and cooperation. It also requires understanding the requirements,

The allocation of high demand, intelligence, reconnaissance, and surveillance resources, such as the RQ-4A Global Hawk, should be based on prioritized requirements.

perceptions, and intelligence policies and procedures of allies and coalition partners and other governmental agencies (OGAs). Unity of effort should maximize the intelligence support provided to the JFC, while simultaneously facilitating information sharing among other appropriate commanders, staffs, OGAs, IGOs, and NGOs supporting the coalition.

6. Prioritization — (Prioritize Requirements Based on Commander's Guidance)

Because operational needs for intelligence often exceed intelligence capabilities, prioritization of collection and analysis efforts and ISR resource allocation are vital aspects of intelligence planning. Prioritization offers a mechanism for addressing requirements and effectively managing risk by identifying the most important tasks and applying available resources against those tasks. Implicit in prioritization is the realization that some intelligence requirements are more important than others. Also implicit is a realization that some lower priority requirements might not be accomplished due to resource limitations. Effective prioritization is absolutely dependent upon active cooperation and coordination between intelligence producers and intelligence consumers.

a. Intelligence consumers drive the intelligence prioritization effort by identifying their intelligence needs and the relative importance of those needs. J-2s advise and assist in this effort by recommending intelligence priorities based on the commander's guidance and operational needs. At the operational and tactical levels, prioritization is driven by the commander's identification of PIRs.

b. An agreed upon prioritization framework provides the basis for optimizing the allocation of limited national ISR resources among combatant commands. The allocation of national ISR resources should be consistent with DIAP established priorities and combatant command PIRs. Without prioritization, competition for ISR resources not only reduces what intelligence could provide, it also inhibits full cooperation among organizations that see themselves as competitors rather than teammates.

7. Excellence — (Strive to Achieve the Highest Standards of Quality)

Producers of intelligence should constantly strive to achieve the highest possible level of excellence in their products. The quality of intelligence products is paramount to the intelligence professional's ability to attain and maintain credibility with intelligence consumers. The **attributes of intelligence product quality** (shown in Figure II-2) are objectives for intelligence activities supporting joint operations and standards against which the quality of intelligence products should be continuously evaluated. To achieve the highest standards of excellence, intelligence products must be:

a. **Anticipatory.** Intelligence must anticipate the informational needs of the commander and joint force staff in order to provide a solid foundation for operational planning and decision making. Anticipating the joint force's intelligence needs requires the intelligence staff to identify and fully understand the command's current and potential missions, the commander's intent, all relevant aspects of the operational environment, and all possible friendly and adversary COAs. Most

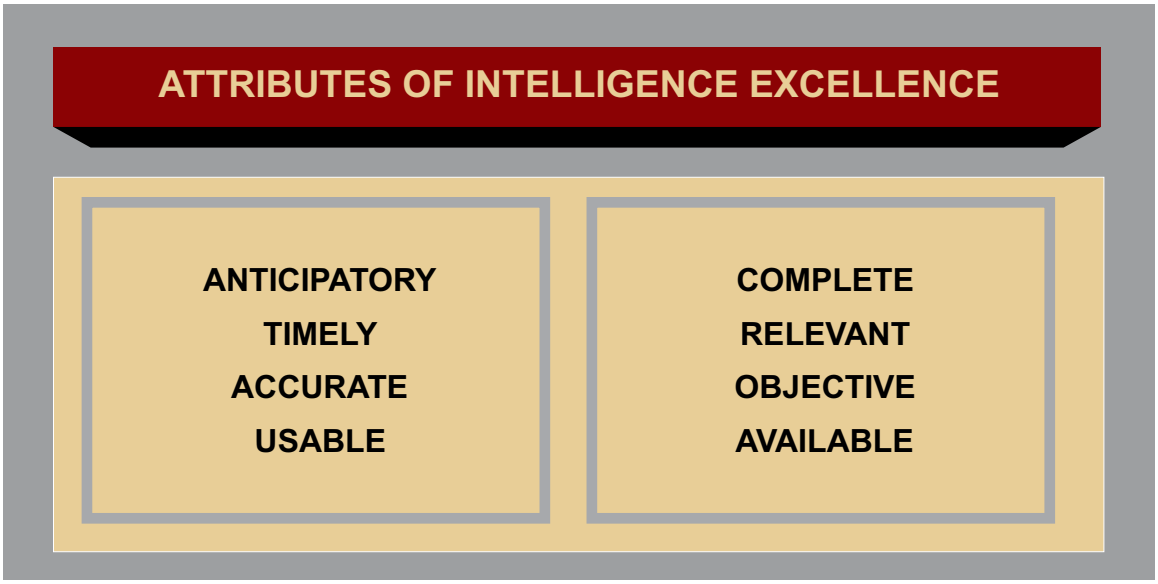


Figure II-2. Attributes of Intelligence Excellence

important, anticipation requires the aggressive involvement of intelligence in operation planning at the earliest time possible.

b. **Timely.** Intelligence must be available when the commander requires it. Timely intelligence enables the commander to anticipate events in the operational area. This, in turn, enables the commander to time operations for maximum effectiveness and to avoid being surprised.

c. **Accurate.** Intelligence must be factually correct, convey an appreciation for facts and the situation as it actually exists, and provide the best possible estimate of the enemy situation and COAs based on sound judgment of all information available. The accuracy of intelligence products may be enhanced by placing proportionally greater emphasis on information reported by the most reliable sources. Source reliability should be evaluated through a feedback process in which past information received from a source is compared with the actual "ground truth" (i.e., when subsequent events, reports, or knowledge confirm the source's accuracy).

d. **Usable.** Intelligence must be tailored to the specific needs of the commander, and must be provided in forms suitable for immediate comprehension. The commander must be able to quickly apply intelligence to the task at hand. Providing useful intelligence requires the producers to understand the circumstances under which their products are used. Commanders operate under mission, operational, and time constraints that will shape their intelligence requirements and determine how much time they will have to study the intelligence that they are provided. Commanders may not have sufficient time to analyze intelligence reports that are excessively complex and difficult to comprehend. The "bottom line" must be up front and easily understandable. Oral presentations should be simple and to the point. The use of approved joint terms and straightforward presentation methods will facilitate rapid and effective application of intelligence to support joint operations.

e. **Complete.** Complete intelligence answers the commander's questions about the adversary to the fullest degree possible. It also tells the commander what remains unknown. To be complete, intelligence must identify all adversary capabilities that may impact mission accomplishment or execution of the joint operation. Complete intelligence informs the commander of all major COAs that are available to the adversary commander, and identifies those assessed as most likely or most dangerous. The effort to produce complete intelligence never ceases. While providing available intelligence to those who need it when they need it, the intelligence staff must give priority to the commander's unsatisfied critical requirements. Intelligence organizations must anticipate and be ready to respond to the existing and contingent intelligence requirements of commanders and forces at all levels of command.

f. **Relevant.** Intelligence must be relevant to the planning and execution of the operation at hand. It must aid the commander in the accomplishment of the command's mission. Intelligence must contribute to the commander's understanding of the adversary, but not burden the commander with intelligence that is of minimal or no importance to the current mission. It must help the commander decide how to accomplish the assigned mission without being unduly hindered by the adversary. Commanders must communicate their intent and their operational concept to the intelligence staff if relevant intelligence is to be produced. Requirements must be updated and refined as the friendly mission or the adversary situation changes.

g. **Objective.** For intelligence to be objective, it should be unbiased, undistorted, and free of prejudicial judgments. The objective analyst must remain open-minded to all hypotheses and should never attempt to make the facts fit preconceptions of a situation or an adversary. In particular, intelligence should recognize each adversary as unique, and should avoid mirror imaging. Red teams should be used to check analytical judgments by ensuring assumptions about the adversary are valid and intelligence assessments are free from mirror imaging and cultural bias.

h. **Available.** Intelligence must be readily accessible to the commander. **Availability is a function of not only timeliness and usability, but also appropriate security classification, interoperability, and connectivity.** Intelligence producers must strive to provide data at the lowest level of classification and least restrictive releasability caveats, thereby maximizing the consumers' access, while ensuring that sources of information and methods of collection are fully protected.

ANALYTIC BIAS: AN ENDURING PROBLEM

1945: **"Furthermore, intelligence officers have sometimes been led in extreme cases into pure crystal-gazing attempts to ascertain enemy intentions on the basis of guess or intuition, unsupported by the available evidence… Playing such hunches is not only dangerous in itself; it leads intelligence officers who have committed themselves to guesses of this kind to look for evidence that will corroborate their views and to depreciate contrary indications."**

Report of the Committee Appointed by the Secretary of War to Study War Department Intelligence Activities, (Lovett Board Report) 5 December 1945

2004: **"The Intelligence Community has long struggled with the need for analysts to overcome analytic biases, that is, to resist the tendency to see what they would expect to see in the intelligence reporting. In the case of Iraq's weapons of mass destruction capabilities, the Committee found that intelligence analysts, in many cases, based their analysis more on their expectations than on an objective evaluation of the information in the intelligence reporting."**

Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq, Select Committee on Intelligence, United States Senate *7 July 2004*

8. Prediction — (Accept the Risk of Predicting Adversary Intentions)

Although intelligence must identify and assess the full range of adversary capabilities, it is most useful when it focuses on the future and adversary intentions. JFCs require and expect timely intelligence estimates that accurately identify adversary intentions, support offensive and/or defense operations, and predict adversary future COAs in sufficient detail as to be actionable. When justified by the available evidence, intelligence should forecast future adversary actions and intentions. If there is inadequate information upon which to base forecasts, the intelligence staff must ensure that the commander is aware of this shortcoming and that the future contains much uncertainty.

a. The intelligence professional must base predictions on solid analysis using proven tools and methodologies. In conventional analysis, the analyst examines, assesses and compares bits and pieces of raw information, and synthesizes findings into an intelligence product that usually reflects enemy capabilities and vulnerabilities. However, predictive analysis goes beyond the identification of capabilities by forecasting enemy intentions and future COAs. As discussed earlier, JIPOE provides an excellent methodology for assessing adversary intentions and predicting the relative probability of enemy COAs.

"In my opinion, a commander is not only entitled to a complete analysis of relative enemy capabilities, but to the views of the intelligence officer as to the most likely one to be anticipated, but of course is at liberty to accept or reject those views."

General Walter Krueger
Commanding General, Sixth US Army
1943-1945

b. Predictive analysis is both difficult and risky (i.e., it challenges the intellectual resources of the analyst while at the same time entailing considerable risk that the events predicted may not come to pass). This type of difficulty and risk apply less to the assessment of adversary capabilities. Predictive analysis is riskier than capabilities analysis because it deals more extensively with the unknown and in some instances must cope with enemy deception plans. Therefore, the chances of analytic failure are greater. As a consequence, there may be a tendency among overly cautious intelligence personnel to avoid predictive analysis. However, JFCs need to know enemy intentions as well as enemy capabilities. **The analyst who successfully performs predictive analysis and accurately assesses enemy intentions in advance of events performs an invaluable service to the commander and staff.**

c. Predictive intelligence is not an exact science and is vulnerable to incomplete information, adversary deception, and the paradox of warning discussed earlier. JFCs must understand that intelligence predictions are only estimates and that they accept an amount of risk in formulating plans based only on the J-2's assessment of the adversary's most probable COA. The J-2 should ensure the JFC is aware of, and has taken into account, all potential adversary COAs and should provide the JFC with an estimate regarding the degree of confidence the J-2 places in each analytic prediction.

9. Agility — (Remain Flexible and Adapt to Changing Situations)

Agility is the ability to shift focus nearly instantaneously and bring to bear the skill sets necessary to address the new problem at hand while simultaneously continuing critical preexisting work. Intelligence structures, methodologies, databases, products, and personnel must be sufficiently agile and flexible to meet changing operational situations, needs, priorities, and opportunities. Whether due to military contingencies or political challenges, sudden changes in the operational environment and requirements of intelligence consumers allow little reaction and recovery time. Therefore, the key to achieving agility is preparation and organization for all contingencies well in advance. Maintaining responsiveness under such circumstances requires considerable vigilance and foresight. Intelligence professionals must anticipate not only the future decisions of adversaries, but of intelligence consumers as well.

a. Achieving agility is fundamentally a long-term project that requires a principled commitment on the part of JFCs and an accurate vision of future requirements. Agility is built only by prior and continuous preparation. JFCs should continuously strive to increase the competence of the intelligence workforce through prior investment in technical training and professional education. Intelligence organizations should be staffed with people who possess an appropriate mix of skills and personal characteristics that enable them to quickly adapt to, and remain responsive in, a changing

operational environment. Intelligence should employ modularized automated data handling and communications systems that are capable of responding to changing circumstances, facilitating survivability, and enabling the seamless delivery of intelligence products to consumers regardless of the conditions in the operational environment. The processes that facilitate these aspects of agility require prior planning and long lead times.

b. Intelligence managers should continuously assess what must be done to support potential requirements, monitor changes in the operational environment, and adjust resources accordingly. Agility requires anticipation and readiness, but for the most part, intelligence organizations should be managed as if they were already "at war" — staffed, equipped, and organized for flexible responses to changing conditions in the operational environment.

10. Collaboration — (Leverage Expertise of Diverse Analytic Resources)

By its nature intelligence is imperfect (i.e., everything cannot be known, analysis is vulnerable to deception, and information is open to alternative interpretations). The best way to avoid these obstacles and achieve a higher degree of fidelity is to consult with, and solicit the opinions of, other analysts and experts, particularly in external organizations.

a. Invaluable expertise on a diverse range of topics resides in governmental and nongovernmental centers of excellence. Likewise, allies and coalition partners often possess in-depth capabilities in either niche or multiple areas and valuable perspectives on diverse intelligence problems. Without collaboration, intelligence products and reports end up being one dimensional and thus less accurate.

b. Intelligence collaboration relies on unhindered access to and sharing of all relevant information and can take many forms such as competitive analysis, brain storming, and federation. Competitive analysis (in which multiple teams use different or competing hypotheses to analyze the same intelligence problem) is useful if sufficient resources are available. In competitive analysis, it is imperative that each team have access to the same information. In situations where competitive analysis is unfeasible, analysts should brainstorm all possible hypotheses with other analysts to gain different perspectives. Collaboration on complex intelligence problems may benefit from a federated approach in which different organizations may assume responsibility for subtopics within the larger problem.

11. Fusion — (Exploit All Sources of Information and Intelligence)

Fusion is the process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity. It draws on the complementary strengths of all intelligence disciplines, and relies on an all-source approach to intelligence collection and analysis.

a. Fusion relies on collection and analysis efforts that optimize the strengths and minimize the weaknesses of different intelligence disciplines. Information is sought from the widest possible range of sources to avoid any bias that can result from relying on a single source of information and to improve the accuracy and completeness of intelligence. The collection of information from multiple sources is essential

to countering the adversary's operations security and deception operations. The operations of all collection sources must be synchronized and coordinated to allow cross-cueing and tip-off among collectors.

LESSON IN FUSION: OPERATION GOLDREGEN

On 1 January 1945, the Luftwaffe conducted an attack (Operation Goldregen) against Allied aircraft located on liberated airfields in Belgium. In a postattack assessment, the intelligence staff of the 12th Army Group Headquarters realized they had received adequate signals intelligence (SIGINT) and human intelligence reporting to have provided tactical warning to the commander. The reports, however had not been fused. Highly compartmented SIGINT (based on Ultra communications intercepts) received before the German attack indicated that an "Operation Goldregen" would be launched. However, the SIGINT specialist had no further knowledge regarding this operation or what it entailed. Filed elsewhere in the headquarters, a prisoner of war interrogation report of a former Luftwaffe clerk in Berlin described aspects of Operation Goldregen — a plan to employ low-flying aircraft in large numbers. This stove-piped compartmentalization of single source intelligence resulted in the unnecessary destruction of several hundred Allied aircraft.

SOURCE: RAND Corporation,
"Notes on Strategic Air Intelligence in World War II,"
October 1949

b. All-source, fused intelligence results in a finished intelligence product that provides the most accurate and complete picture possible of what is known about an activity. While the level of detail in single-source reports may be sufficient to meet narrowly defined customer needs, fused reports are essential to gain an in-depth understanding. Because the adversary will engage in deception efforts, analysts should guard against placing unquestioned trust in a single-source intelligence report.

CHAPTER III
INTELLIGENCE ORGANIZATIONS AND RESPONSIBILITIES

"The necessity of procuring good Intelligence is apparent and need not be further urged."

General George Washington *26 July 1776*

1. Defense Intelligence and the Intelligence Community

A wide variety of intelligence organizations exist at the national and theater levels that are capable of providing support to joint operations. During most joint operations, JFCs will require not only military intelligence, but also intelligence on nonmilitary aspects of the operational environment such as economic, informational, social, political, diplomatic, biographic, human factors, and other types of intelligence. Equally important is knowledge of how all these aspects interrelate to form a systems perspective of the adversary and other relevant aspects of the operational environment. In order to efficiently exploit the wide range of knowledge and other intelligence expertise resident in both DOD and non-DOD members of the IC, JFCs and their J-2s should understand the national intelligence structure as well as respective roles and responsibilities of theater and national intelligence organizations. This is increasingly important as new technology facilitates collaborative analysis and production throughout the IC, thus blurring the traditional distinction between joint and national-level intelligence operations.

a. National Intelligence Leadership Structure

(1) **The Director of National Intelligence** (DNI) has overall responsibility for intelligence support to the President and the day-to-day management of the IC. Specifically, the DNI establishes objectives and priorities for the IC and manages and directs the tasking of national intelligence collection, analysis, production, and dissemination. The DNI also develops and determines the annual budget for the National Intelligence Program (NIP) and monitors the implementation and execution of the NIP by the heads of IC member organizations. The DNI implements policies and procedures to ensure all-source intelligence includes competitive analysis and that alternative views are brought to the attention of policy makers. Additionally, the Office of the DNI exercises control over the National Intelligence Council, National Counterintelligence Executive, National Counterterrorism Center, and National Counterproliferation Center, and has authority to establish additional national intelligence centers when deemed necessary to address other intelligence priorities, such as regional issues.

(2) **The Under Secretary of Defense for Intelligence (USD(I))** is the principal staff assistant and advisor to the Secretary of Defense on all intelligence, CI and security, and other intelligence-related matters. On behalf of the Secretary of Defense, the USD(I) exercises authority, direction, and control of intelligence and CI organizations within DOD to ensure that they are manned, trained, equipped, and organized to support DOD missions and are responsive to DNI requirements.

(3) **The Director of the Defense Intelligence Agency** advises the Secretary of Defense and Deputy Secretary of Defense, Chairman of the Joint Chiefs of Staff, CCDRs, and USD(I) on all matters concerning military and military-related intelligence and is the principal DOD intelligence representative in the national foreign intelligence process. The Director of DIA also serves in several additional capacities. As Director, Defense Joint Intelligence Operations Center (DJIOC), the Director coordinates intelligence support to meet combatant command requirements and reports to the Secretary of Defense through the Chairman of the Joint Chiefs of Staff. The Director also commands the United States Strategic Command's (USSTRATCOM's) Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance (JFCC-ISR) which is integrated with the DJIOC and oversees the coordination of global ISR in support of DOD worldwide military operations. Finally, the Director serves as the Defense HUMINT Manager and is responsible for coordinating all DOD HUMINT resources and requirements.

(4) **The Chairman of the Joint Chiefs of Staff** provides direction to the Joint Staff Director for Intelligence, J-2, to ensure that adequate, timely, and reliable intelligence and CI support is available to the Joint Chiefs of Staff and the combatant commands.

(5) **The Joint Staff Directorate for Intelligence, J-2,** is a unique organization, in that it is both a major component of DIA (a combat support agency) and a fully integrated element of the Joint Staff. The J-2 provides continuous intelligence support to the Chairman of the Joint Chiefs of Staff, Joint Staff, National Military Command Center (NMCC), and combatant commands in the areas of global I&W and crisis intelligence. The J-2, in cooperation with other DIA elements, provides strategic warning, threat assessments and intelligence-related advice to the Chairman of the Joint Chiefs of Staff. It also exercises staff supervision of the intelligence alert center supporting the NMCC and keeps the Chairman of the Joint Chiefs of Staff apprised of foreign situations that are relevant to current and potential national security policy, objectives, and strategy. During crises, the intelligence support to the NMCC expands as necessary by utilizing DIA assets to form a working group, intelligence task force or, in the case of a major crisis, an expanded intelligence task force. The Joint Staff J-2 is also responsible for representing and advocating combatant command views and intelligence requirements to the Joint Staff and Office of the Secretary of Defense (OSD). The Joint Staff J-2 is also responsible for coordinating with the combatant commands and the DJIOC in staffing all intelligence-related Chairman of the Joint Chiefs of Staff orders (e.g., alert orders, planning orders, warning orders) and RFFs.

(6) **The Chiefs of the Military Services and their Service intelligence and CI chiefs and staffs** provide intelligence and CI support for departmental missions related to military systems, equipment, and training. They also support national intelligence activities in support of DOD entities, including combatant commands, subordinate joint commands, and Service components of those commands. Service intelligence staffs and organizations produce a broad array of products and services (such as weapons system-specific targeting materials) as well as technical expertise in specialized areas such as IO and foreign weapons systems. At both the component and unit level, Service intelligence personnel are involved in the operation of ISR assets and provide tailored intelligence support for weapons system employment.

b. **The Intelligence Community.** The IC consists of the 16 member organizations depicted in Figure III-1. Both DOD and non-DOD members of the IC routinely provide support to JFCs while

continuing to support national decision makers. However, the focus of national organizations is not evenly split among intelligence customers and varies according to the situation and competing requirements as prioritized by the national intelligence leadership.

(1) **Military Members of the Intelligence Community.** The military members of the IC consist of the four defense agencies and the four Service intelligence centers discussed below. The Secretary of Defense and USD(I) supervise the DOD portion of the IC and are assisted in their intelligence management responsibilities by the ISR Integration Council and the Military Intelligence Board (MIB). The ISR Integration Council assists the USD(I) with respect to matters relating to the integration of ISR capabilities and the coordination of related developmental activities of DOD components and combatant commands. The MIB serves as the senior "board of governors" for the DOD portion of the IC and works to develop cooperation and consensus on combat support agency, Service, and combatant command intelligence issues.

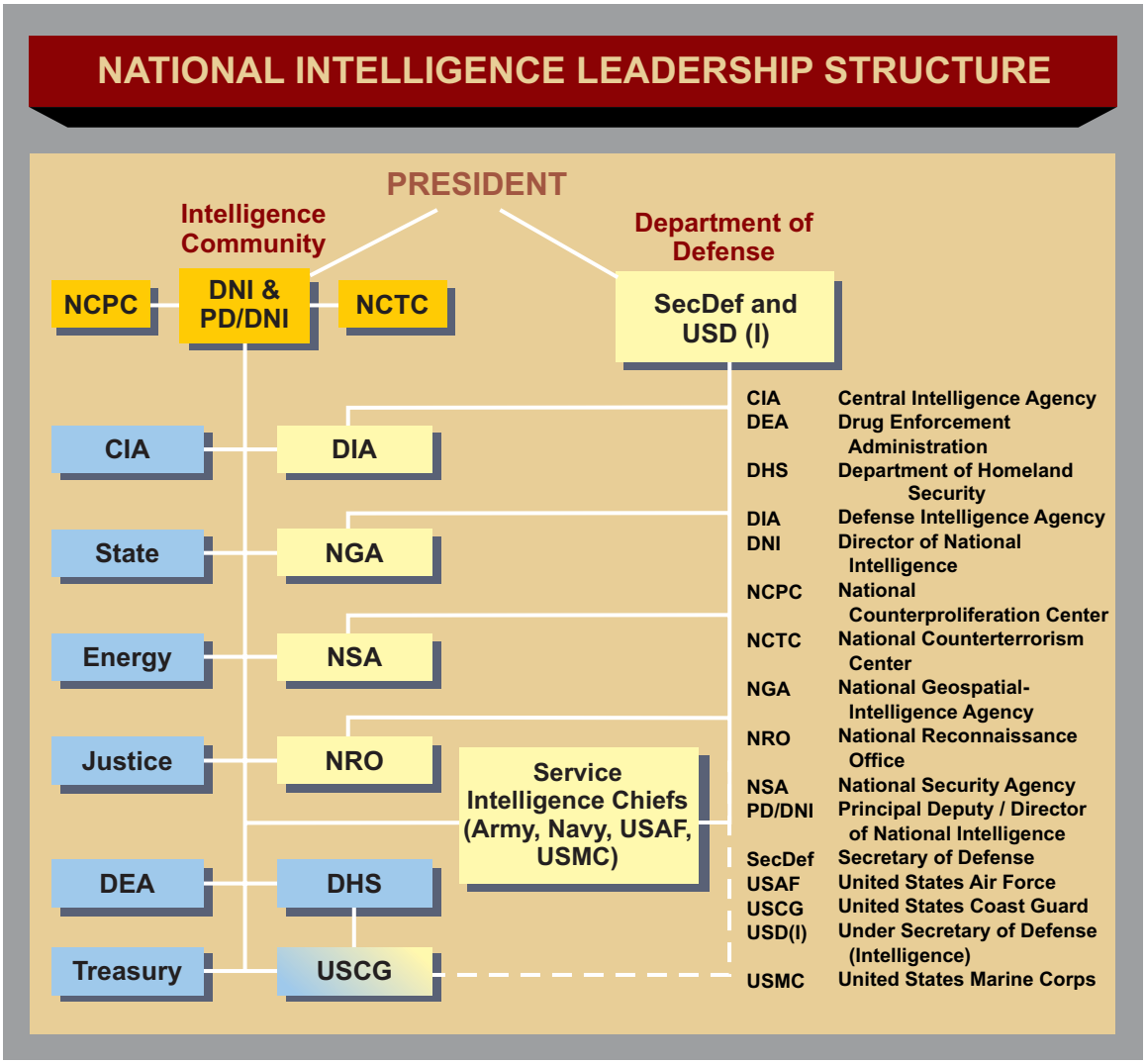


Figure III-1. National Intelligence Leadership Structure

(a) **Defense Intelligence Agency.** DIA has oversight of the DIAP and provides intelligence support in areas such as: all-source military analysis, human factors analysis, HUMINT, MASINT, MEDINT, CI, counterterrorism, CBRNE counterproliferation, counterdrug operations, IO, personnel recovery, peacekeeping and coalition support, noncombatant evacuation operations, I&W, targeting, battle damage assessment (BDA), current intelligence, systems analysis of the adversary, collection management, intelligence architecture and systems support, intelligence support to operation planning, defense critical infrastructure protection, and document and media exploitation.

(b) **National Security Agency (NSA)/Central Security Service (CSS).** NSA/CSS is a unified organization structured to provide for the SIGINT mission of the United States and to ensure the protection of national security systems for all departments and agencies of the US Government.

(c) **National Geospatial-Intelligence Agency.** NGA provides timely, relevant, and accurate GEOINT support to include imagery intelligence (IMINT), geospatial information, national imagery collection management, commercial imagery, imagery-derived MASINT, and some meteorological and oceanographic data and information.

(d) **National Reconnaissance Office (NRO).** NRO is responsible for integrating unique and innovative space-based reconnaissance technologies, and the engineering, development, acquisition, and operation of space reconnaissance systems and related intelligence activities.

(e) **US Army Intelligence.** The Army Deputy Chief of Staff for Intelligence exercises staff supervision over the US Army Intelligence and Security Command (INSCOM). INSCOM, which includes the National Ground Intelligence Center, provides intelligence support to strategic- and operational-level commanders in the areas of IMINT, MASINT, SIGINT, operational and tactical HUMINT, CI, IO, GMI, and scientific and technical intelligence (S&TI). Other organizations include the Army Reserve Military Intelligence Readiness Command.

(f) **US Navy Intelligence.** The Director of Naval Intelligence exercises staff supervision over the Office of Naval Intelligence (ONI), which provides the intelligence necessary to plan, build, train, equip, and maintain US naval forces. The National Maritime Intelligence Center consists of ONI, the US Coast Guard (USCG) Intelligence Coordination Center, the Navy Information Operations Command, and detachments of the Marine Corps Intelligence Activity (MCIA) and Naval Criminal Investigative Service.

(g) **US Air Force Intelligence.** The Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance is responsible for intelligence policy, planning, programming, evaluation, and resource allocation. The Air Force's main production facility is the National Air and Space Intelligence Center. Primary collection, analysis, and production units are organized under the Air Combat Command, the Air Force Warfare Center, and the Air Force Intelligence, Surveillance, and Reconnaissance Agency. Additionally, the Air Force Office of Special Investigations is the Service's main focal point for CI activities.

(h) **US Marine Corps Intelligence.** The Director of Intelligence is the Commandant's principal intelligence staff officer and the functional manager for intelligence, CI, and cryptologic material. The Director exercises staff supervision of the MCIA, which provides tailored intelligence products to support Marine Corps operating forces, and serves as the fixed site of the Marine Corps Intelligence Surveillance and Reconnaissance Enterprise.

(2) **Nonmilitary Members of the Intelligence Community.** Joint operations require knowledge of both military and nonmilitary aspects of the operational environment. Much of this expertise falls outside the purview of the DOD members of the IC. JFCs and their J-2s should be familiar with the roles and responsibilities of the following non-DOD members of the IC.

(a) **Central Intelligence Agency (CIA).** CIA's primary areas of expertise are in HUMINT collection, all-source analysis, and the production of political, economic, and biographic intelligence.

(b) **Department of State (DOS).** The DOS Bureau of Intelligence and Research performs intelligence analysis and production on a wide range of political and economic topics essential to foreign policy determination and execution.

(c) **Department of Energy (DOE).** DOE analyzes foreign information relevant to US energy policies and nonproliferation issues.

(d) **Federal Bureau of Investigation (FBI).** The FBI has primary responsibility for CI and counterterrorism operations conducted in the United States. The FBI shares law enforcement and CI information with appropriate DOD entities and combatant commands.

(e) **Department of the Treasury.** The Department of the Treasury analyzes foreign intelligence related to economic policy and participates with DOS in the overt collection of general foreign economic information.

(f) **United States Coast Guard.** The USCG operates as both a military service and a law enforcement organization and provides general maritime intelligence support to commanders from the strategic to tactical level in the areas of HUMINT, SIGINT, GEOINT, MASINT, OSINT, and CI.

(g) **Department of Homeland Security.** The Directorate for Information Analysis and Infrastructure Protection analyzes the vulnerabilities of US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to the Homeland Security Advisory System.

(h) **Drug Enforcement Administration.** The Office of National Security Intelligence collects and analyzes information related to illegal drug production, smuggling, and trafficking.

JP 2-01, Joint and National Intelligence Support to Military Operations, *provides details of the support that national agencies such as DIA, CIA, NSA, NRO, and NGA, as well as the intelligence organizations of the Services, can provide to joint forces.*

2. Defense and Joint Intelligence Organizations

In addition to the J-2 staffs at every joint level of command, the key organizations in the defense intelligence architecture are the DJIOC, the combatant command joint intelligence operations centers (JIOCs), the JTF joint intelligence support elements (JISEs), national intelligence support teams (NISTs), JFCC-ISR, and the joint intelligence reserve centers (JRICs). At the JTF level, a joint intelligence support element (JISE) is normally established; however a JIOC may be established at the direction of the JFC based on the scope, duration, and mission of the unit or JTF. For the remainder of this document "JISE" will be used as the standard term to describe the intelligence organization at the JTF-level. Working together, these organizations play the primary role in managing and controlling the various types of intelligence functions and operations that comprise the intelligence process described in Chapter I, "The Nature of Intelligence." These organizations are linked by formal relationships that facilitate RFI management, optimize complementary intelligence functions by echelon, and promote the timely flow of critical intelligence up, down, and laterally. In addition to the support provided by joint intelligence staffs and organizations, JFCs receive valuable support from the Service intelligence organizations and from the intelligence staffs and organizations belonging to the joint force components. JFCs must consider the intelligence capabilities of these elements during the planning and execution of all joint operations. Separate intelligence units and organizations assigned to the joint force will receive one of the intelligence support missions (shown in Figure III-2) from the JFC. Intelligence staffs and forces organic to a component command will remain the assets of that component commander. If the JFC wants the organic intelligence assets of a component to support other units, the JFC will usually assign an intelligence support mission to that component commander.

Support relationships are further explained in JP 1, Doctrine for the Armed Forces of the United States.

a. **Defense Joint Intelligence Operations Center.** The DJIOC is the lead DOD intelligence organization responsible for integrating and synchronizing military intelligence and national intelligence capabilities. It plans, prepares, integrates, directs, synchronizes, and manages continuous, full-spectrum DOD intelligence operations in support of the combatant commands. The DJIOC collaborates with USSTRATCOM's JFCC-ISR and DNI representatives to formulate and recommend to the Chairman of the Joint Chiefs of Staff, for Secretary of Defense action, solutions for deconflicting combatant command requirements for national intelligence resources, and ensures an integrated response to their needs. It ensures that joint force crisis-related and time-sensitive intelligence requirements are tasked to the appropriate Service, combatant command or national agency, when the requirements cannot be satisfied by assigned or attached assets. The DJIOC may also propose permanent realignment of intelligence resources among combatant command JIOCs to support long-term shifts in defense priorities. Proposals for permanent realignment of resources must be coordinated with the Joint Staff, appropriate combatant commands and combat support agencies and forwarded to the Chairman of the Joint Chiefs of Staff for action by the Secretary of Defense, who will coordinate with the DNI as appropriate. DJIOC functions include:

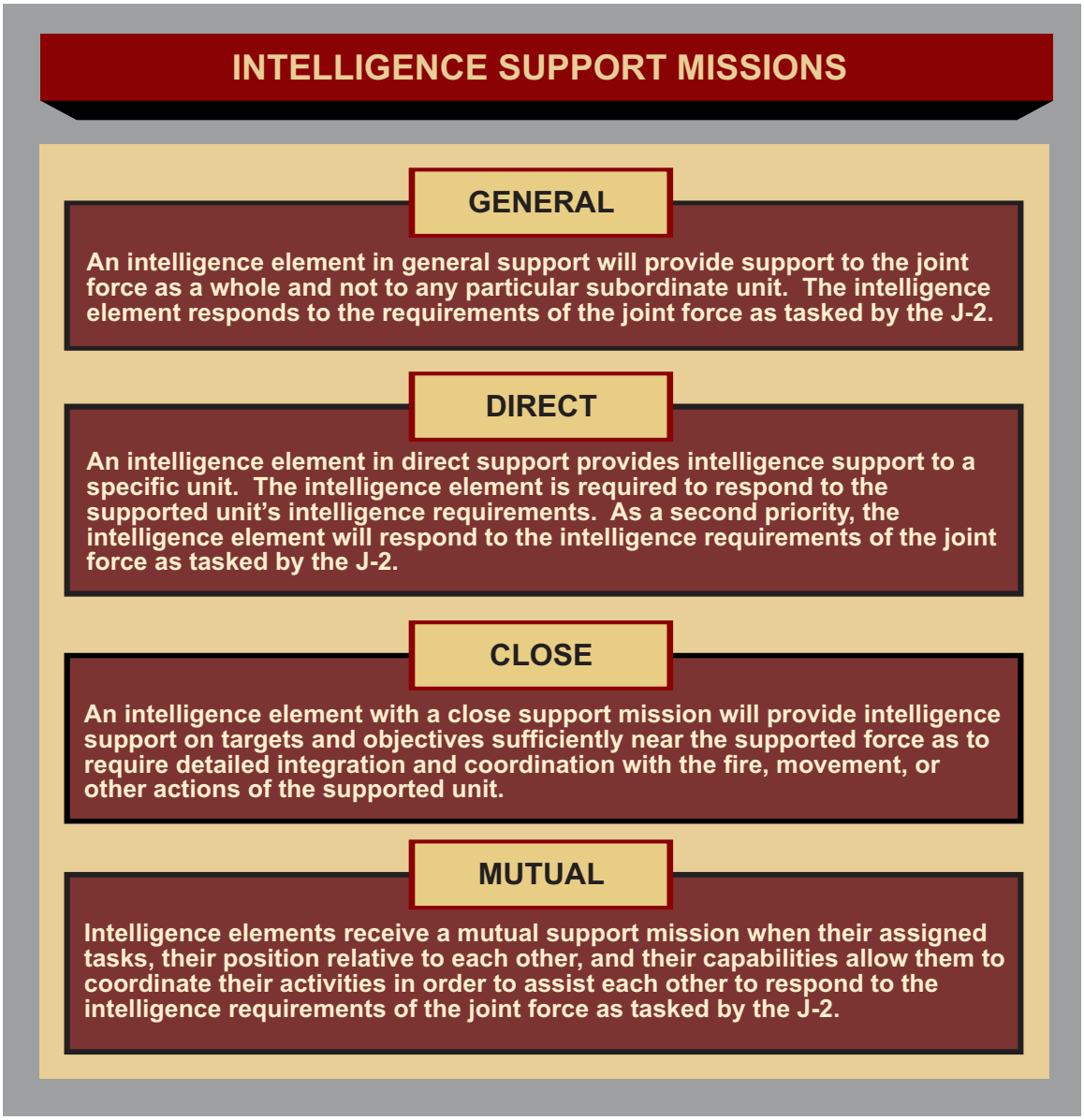


Figure III-2. Intelligence Support Missions

(1) Formalizing and implementing an intelligence planning process, under the guidance and oversight of the USD(I) and the Chairman of the Joint Chiefs of Staff, to support joint operation planning. Synchronizing intelligence planning activities to support the development and execution of annex B of the combatant command's OPLANs or concept plans (CONPLANs) and coordinating all national-level intelligence planning with the DNI.

(2) Providing combatant command JIOCs with the full spectrum of management recommendations on issues related to ISR requirements, management, exploitation, and evaluation.

(3) Assessing and evaluating defense intelligence tasks to determine risk, identify mitigation strategies, and develop recommendations for reprioritization and realignment of intelligence resources.

(4) Serving as an advocate for combatant command intelligence requirements and JIOC capabilities.

(5) Managing NISTs to provide timely, tailored, national-level, all-source intelligence to combatant commands during crisis and contingency operations.

(6) Orchestrating national intelligence support to major combatant command exercises.

(7) Coordinating and prioritizing intelligence requirements across combatant commands and among the DOD members of the IC. The DJIOC's coordination responsibilities include:

(a) Maintaining awareness of intelligence requirements and ongoing intelligence operations.

(b) Evaluating competing requirements and requests for additional support.

(c) Developing proposed alternatives in collaboration with the Joint Staff, combatant commands, combat support agencies, and capability providers.

(d) Forwarding alternatives to the Chairman of the Joint Chiefs of Staff for approval by the Secretary of Defense in coordination with the DNI as appropriate.

(e) Monitoring task execution and optimizing the use of analytical resources among the DOD members of the IC.

(f) Coordinating with each combatant command JIOC or J-2 to ensure it receives adequate reachback support from national intelligence resources.

b. **Combatant Command Joint Intelligence Operations Centers.** The combatant command JIOCs are the primary intelligence organizations providing support to joint forces at the operational and tactical levels. The JIOC integrates the capabilities of DNI, Service, combat support agency, and combatant command intelligence assets to coordinate intelligence planning, collection management, analysis, and support. The JIOC construct seamlessly combines all intelligence functions, disciplines, and operations into a single organization, ensures the availability of all sources of information from both combatant command and national intelligence resources, and fully synchronizes and integrates intelligence with operation planning and execution. Although a particular JIOC cannot be expected to completely satisfy every RFI, it can coordinate support from other intelligence organizations; lower, higher, and laterally.

(1) Each combatant command structures its JIOC in accordance with the needs and guidance of the CCDR. The JIOC construct is intended to facilitate the agile management of all intelligence functions, disciplines, and operations according to the principle of "centralized planning and direction — decentralized execution." During noncrisis periods, JIOC personnel levels are normally maintained to the degree required to perform essential functions such as I&W, current intelligence, collection management, and GMI production (to include systems analysis of the adversary and other

relevant aspects of the operational environment), in the JIOC's area of production responsibilities. During crises, the JIOC can be augmented with personnel from organizations of other combatant commands, other commands, Reserve components, and national intelligence organizations, according to the needs of the CCDR. The JIOC normally leverages national intelligence capabilities through the CCDR's DNI representative, interagency representatives, and/or DJIOC forward element (DFE) - DJIOC personnel that are forward deployed to the combatant command JIOC in a direct support relationship. The DFE helps the combatant command JIOC translate intelligence requirements into DJIOC intelligence support tasks, and facilitates the leveraging of DIA analytical efforts to support the command.

(2) For combatant commands having a JIOC construct which includes staff functions (e.g., operations and/or planning) in addition to intelligence, the CCDR is responsible for determining and specifying the respective roles, responsibilities, and relationships between the combatant command J-2 and the JIOC. In such cases, whether or not designated as chief of the JIOC, the J-2 shall retain authority to manage and direct all military intelligence personnel and resources assigned to the combatant command.

(3) The combatant command's JIOC ensures intelligence needs of the command and subordinate joint force and component commands are satisfied in accordance with command priorities. Functions of the JIOC may include, but are not limited to:

(a) Coordinating the intelligence effort of subordinate joint force commands.

(b) Coordinating the theater collection plan and employment of theater assigned and supporting sensors.

(c) Developing and maintaining databases that support planning, operations, and targeting.

(d) Validating assessments from higher, lower, and adjacent sources.

(e) Conducting ISR visualization and participating with J-3 in the dynamic management of ISR assets.

(f) Submitting national collection requirements to the combatant command DNI representative.

(g) Coordinating with J-3 to ensure intelligence is fully synchronized and integrated with operations.

(h) Coordinating with J-5 to ensure intelligence is fully synchronized and integrated with plans.

(i) Conducting all-source intelligence analysis and production in support of joint force and component command requirements.

(j) Employing red teams to address the CCDR's most pressing intelligence and operational issues from the adversary's perspective.

(k) Serving as the focal point for intelligence planning.

c. **Joint Task Force Joint Intelligence Support Elements.** At the discretion of a subordinate JFC, a JTF JISE may be established during the initial phases of an operations to augment the subordinate joint force J-2 element. Under the direction of the joint force J-2, a JTF JISE normally manages the intelligence collection, production, analysis, and dissemination for a joint force.

(1) **The size and organization of the JISE will be determined by the JFC** based upon the recommendation of the J-2 and available resources. Personnel and equipment requirements for the JISE, including augmentation, are submitted to the combatant command. Resources will be provided through the RFF process.

(2) **When formed, the JTF JISE may be collocated with the JTF J-2 element in the joint operations area (JOA), or may operate in a "split base" mode.** In split-base mode, the JISE's operations and personnel are divided between two locations: with the JTF J-2 in the JOA, and outside the JOA, possibly at the JTF's home base or at another remote location. Split-base operations may reduce the number of personnel deployed and supported in the JOA and the attendant communication system infrastructure thus reducing potential force protection issues.

(3) The JTF J-2 defines the JISE's functions and responsibilities and its relationship with the J-2 staff. In many cases, specific responsibilities may be shared between the J-2 staff and JISE.

(4) Any JTF requirements for captured materiel and document exploitation support are submitted via the combatant command JIOC to the DJIOC for coordination with DIA and the Service intelligence centers. The support is tailored to the crisis and can range from a liaison officer to the joint force J-2, to a robust joint staff element with a fully staffed joint captured materiel exploitation center and joint document exploitation center.

d. **National Intelligence Support Team.** At the request of a CCDR, the DJIOC coordinates the deployment of a NIST to support a commander, JTF. The NIST is a nationally sourced team composed of intelligence analysts and communications experts from DIA, CIA, NGA, NSA, and other IC agencies as required. During crisis or contingency operations, it provides commanders with a tailored, national-level, all-source intelligence team, ranging from a single agency element with limited ultra-high frequency voice connectivity to a fully equipped, multiagency team with joint deployable intelligence support system (JDISS) and Joint Worldwide Intelligence Communications System (JWICS) video-teleconferencing capabilities. A NIST typically supports intelligence operations at the JTF headquarters and is traditionally collocated with the JTF J-2; although, the DJIOC portion of the NIST has the capability to go forward as required. Current modes of operation rely on both agency and command-provided communications (i.e., equipment and bandwidth) to support deployed NIST elements.

A deployed military interrogation team questions villagers during Operation Mountain Sweep in Afghanistan.

The NIST provides commanders with analytical expertise, I&W, special assessments, and targeting support (when the United States Joint Forces Command (USJFCOM) Quick Reaction Team (QRT) is present). In direct support of the JTF, the NIST performs functions as designated by the JTF J-2, provides access to national databases, and facilitates RFI management.

e. **United States Joint Forces Command's Quick Reaction Team.** USJFCOM maintains a standing QRT for the provision of targeting and collection support to combatant commands. The QRT deploys from USJFCOM when requested by a combatant command to support crisis or contingency operations. The DJIOC coordinates and validates all requests for augmentation by USJFCOM QRT personnel. QRT personnel are integrated into the JTF intelligence structure to provide enhanced targeting and collection management support.

f. **United States Strategic Command's JFCC-ISR.** In support of USSTRATCOM's Unified Command Plan-assigned ISR mission, JFCC-ISR plans, integrates and coordinates defense global ISR strategies in support of joint operation planning and combatant command planning/operations. JFCC-ISR formulates recommendations to integrate global ISR capabilities associated with the missions and requirements of DOD ISR assets in coordination with the DJIOC and Commander, USSTRATCOM. In coordination with the combatant commands, JFCC-ISR provides personnel and resources in direct support of the combatant command JIOCs.

g. **Joint Reserve Intelligence Center (JRIC).** A JRIC is a joint intelligence production and training activity that uses information networks to link reservist intelligence personnel with the combatant commands, Services, and/or combat support agencies. A JRIC is located within a Service-owned and

managed sensitive compartmented information (SCI) facility and may also include surrounding collateral and unclassified areas involved in the performance and direct management of intelligence production work that uses Joint Reserve Intelligence Program infrastructure and connectivity. The more than 20 JRICs located around the country are equipped to effectively serve as satellite elements to combatant command JIOCs, however they are shared facilities that serve multiple customers and missions.

3. Intelligence Federation

During crises, joint forces may also garner support from the IC through intelligence federation. Intelligence federation enables combatant commands to form support relationships with other theater JIOCs, Service intelligence centers, JRICs, or other DOD intelligence organizations to assist with the accomplishment of the joint force's mission. These support relationships, called federated partnerships, are preplanned agreements (formalized in OPLANs, national intelligence support plans, or memorandums of agreement) intended to provide a rapid, flexible, surge capability enabling personnel from throughout the IC to assist the combatant command while remaining at their normal duty stations. Federated support can be provided in specific functional areas directly related to the crisis, or by assuming temporary responsibility for noncrisis-related areas within the combatant command's areas of responsibility (AORs), thereby freeing the supported command's organic assets to refocus on crisis support.

Detailed guidance on intelligence federation planning and support is discussed in JP 2-01, Joint and National Intelligence Support to Military Operations.

4. Command and Staff Intelligence Responsibilities

a. **Joint Force and Component Commander Responsibilities.** JFCs and their component commanders are more than just consumers of intelligence. Commanders are the key players in the planning and conduct of intelligence operations. JFCs organize their joint force staff and assign responsibilities as necessary to ensure unity of effort and mission accomplishment. Additionally, commanders (as well as other users) must continuously provide feedback on the effectiveness of intelligence in supporting operations. Figure III-3 depicts commanders' intelligence responsibilities.

(1) **Understand Intelligence Doctrine, Capabilities, and Limitations.** Commanders must know intelligence doctrine and understand intelligence discipline capabilities and limitations as well as procedures and products. Most important, commanders should understand that intelligence analysis provides only estimates of an adversary's probable intention and most likely future COA — they do not determine the actual course of future events. Although intelligence provides a necessary basis for operation planning, it can never be perfect, and operation planning based on intelligence will always entail a degree of risk.

(2) **Provide Planning Guidance.** Commanders focus the planning process through the commander's intent, planning guidance, and initial CCIR. The commander's guidance provides the basis for the formulation of PIRs, the concept of intelligence operations, and coherent target development and target nominations.

Figure III-3. Commanders' Intelligence Responsibilities

(3) **Define the Area of Interest.** Commanders should define their areas of interest based on mission analysis, their concept of operations (CONOPS), and a preliminary assessment of relevant aspects of the operational environment (prepared as part of the JIPOE process).

(4) **Identify Critical Intelligence Needs.** Commanders should identify their CCIRs, to include PIRs, as early as possible in order to facilitate intelligence planning and synchronization with operations. Commanders should not only specify what information is needed, but also when it is needed in order to be integrated into operation planning. Commanders should understand that in some situations, their PIRs will require ISR support from higher echelons that may entail substantial lead time.

(5) **Integrate Intelligence in Plans and Operations.** Commanders are ultimately responsible for ensuring that intelligence is fully integrated into their plans and operations. The successful synchronization of intelligence operations with all other elements of joint operations occurs in the JIOC and begins with commanders involving their intelligence planners in the earliest stages of the joint operation planning process.

(6) **Proactively Engage the Intelligence Staff.** Commanders should actively engage their intelligence officers in discussions of adversaries, force protection, and future operations. Frequent consultations between the JFC and the joint force's intelligence staff facilitate situational awareness, particularly a mutual understanding regarding the interaction between friendly and adversary systems.

"Nothing is more worthy of the attention of a good general than the endeavor to penetrate the designs of the enemy."

Machiavelli Discourses, 1517

(7) **Demand High Quality, Predictive Intelligence.** Commanders must hold their intelligence personnel accountable for providing predictive intelligence that meets all the attributes of intelligence excellence discussed earlier. However, JFCs must also understand the challenges and limitations that confront intelligence personnel in assessing adversary intentions and future COAs.

b. **Joint Force J-2 Responsibilities.** The J-2 assists the JFC in developing strategy, planning operations and campaigns, and tasking intelligence assets, for effective joint and unified operations. Additionally, the J-2 is responsible for determining the requirements and direction needed to ensure unity of the intelligence effort and to support the commander's objectives. The combatant command J-2 provides higher echelons, up to and including the DJIOC, and subordinate commands with a single, coordinated intelligence picture by fusing national and theater intelligence into all-source estimates and assessments. The combatant command J-2's responsibility also includes applying national intelligence capabilities, optimizing the utilization of joint force intelligence assets, and identifying and integrating additional intelligence resources. The scope of needs, resources, and procedures will depend on the mission, nature, and composition of the force. To plan, coordinate, and execute required intelligence operations, joint force J-2s have the following major responsibilities (See Figure III-4).

(1) **Provide Threat Assessments and Warning.** The J-2 is responsible for analyzing all relevant aspects of the operational environment, determining adversary capabilities, and estimating adversary intentions. The J-2 provides the resulting threat assessments and warning to the joint force and its components in a manner consistent with the intelligence principle of excellence (i.e., the product must be anticipatory, timely, accurate, usable, complete, relevant, objective and available).

(2) **Participate in all Decision-Making and Planning.** Using JIPOE as a basis, the J-2 participates in the JFC's decision-making and planning processes from the time that operations are first contemplated or directed until the completion of the operation. The JFC and the J-2 must conduct a continuous dialog concerning the adversary's relative strengths, weaknesses, and ability to prevent the joint force from accomplishing its mission.

(3) **Synchronize Intelligence With Operations and Plans.** The J-2 must ensure that intelligence collection, processing, exploitation, analysis and dissemination activities are planned, sequenced, and timed to support the commander's decision making process and to meet the requirements of planners. This is particularly important in the field of target intelligence, which provides a functional link between intelligence and operations. The commanders' desired effects provide the basis for target development, nomination and prioritization, while assessment will inform any changes in the commander's objective and strategy.

(4) **Formulate Concept of Intelligence Operations.** To communicate guidance and requirements to higher and lower echelons of command, the joint force J-2 develops and disseminates a concept of intelligence operations. The concept can include such information as tasking authorities, reporting responsibilities, required coordination, obtaining communications-related support and backups, and requirements for intelligence-related boards, centers, and teams.

Figure III-4. Joint Force J-2 Responsibilities

For further information regarding the concept of intelligence operations see JP 3-33, Joint Task Force Headquarters, *and JP 2-01*, Joint and National Intelligence Support to Military Operations.

(5) **Develop Detailed Intelligence Annexes.** The JFC's PIRs and the results of wargaming serve as the basis for the intelligence annex of each directed OPLAN and CONPLAN. The annex will list the JFC's PIRs and the supporting information requirements. It will identify the intelligence forces available for the operation, resolve shortfalls, and assign or recommend tasks (as appropriate) that will best support the joint force's requirements. This annex should allocate available joint force and supporting intelligence assets among the elements of the joint force in accordance with the commander's intent, main effort, and CONOPS. The J-2 must ensure that component intelligence requirements critical to success of key component operations receive appropriate intelligence support. The annex also addresses how any shortfalls between assigned or attached capabilities and requirements will be met by national and supporting capabilities.

(6) **Integrate National and Theater Intelligence Support.** The J-2 must plan for integrating national and theater intelligence elements and products into the joint force's intelligence structure. National and theater intelligence organizations will make operations feasible that could not be accomplished without their access, capability, capacity, or expertise.

Intelligence support to joint operation planning is discussed in greater detail in Chapter IV, "Intelligence Support to Planning, Executing, and Assessing Joint Operations."

(7) **Exploit Combat Reporting from Operational Forces.** Forward and engaged combat forces have a responsibility to report information that can be integrated with intelligence obtained from

reconnaissance and surveillance assets. In many situations, even negative reporting from operational forces may be valuable (e.g., a lack of contact with adversary forces may be just as significant as positive contact). Likewise, special operations forces (SOF) provide the JFC with a unique manned and unmanned "eyes-on-target" deep look capability, especially useful in areas where other sensors are not available, or can't provide required "resolution." Based on operational requirements, the J-2 must identify the PIRs and associated reporting criteria to properly focus SOF assets.

(8) **Organize for Continuous Operations.** Intelligence organizations should be structured for continuous day-night and all-weather operations. The J-2's concept of intelligence operations should provide for continuity of support even if communications are severely stressed or temporarily lost. Intelligence resources, activities, and communications must be structured and operated to be sufficiently survivable to ensure required intelligence support is available to the JFC. An important component of survivability is redundancy in critical intelligence architectural components and capabilities.

(9) **Ensure Accessibility of Intelligence.** The J-2 must ensure that intelligence is readily accessible throughout the joint force while still adhering to security standards (e.g., security clearance and need-to-know requirements). All efforts must be made to ensure that the personnel and organizations that need access to required intelligence will have it in a timely manner. When operating in a coalition environment, personnel experienced with foreign disclosure regulations should be assigned to the joint force to facilitate the efficient flow of intelligence to authorized coalition members.

(10) **Establish a Joint Intelligence Architecture.** A truly joint intelligence infrastructure must be created to provide the best possible intelligence to the JFC. It must be constructed to ensure protection of information and intelligence from inadvertent disclosure, and guarantee integrity of the data and assured access to all sources. The joint force intelligence architecture required to support the JFC's concept of operation must be designed during the intelligence planning process and refined during the pre-deployment phase. JTFs that are primarily composed of forces from a single Service should be provided the necessary personnel and communications to permit the implementation of a joint intelligence system.

Intelligence architecture requirements are discussed in greater detail in Chapter V, "Joint, Interagency, and Multinational Intelligence Sharing and Cooperation."

THE COMMANDER'S INTELLIGENCE RESPONSIBILITIES

In June 1942, Admiral Sir Dudley Pound (First Sea Lord of the Admiralty), fearing an attack by the German battleship Tirpitz, ordered the Royal Navy cruisers and destroyers escorting the Murmansk bound Convoy PQ17 to abandon the convoy while it was off the North Cape of Norway. The convoy was further ordered to scatter. Each ship was to make its own way to Murmansk.

Admiral Pound ordered the convoy to disperse despite Commander N.E. Denning's (the Admiralty's Operational Intelligence Centre (OIC) German surface ship section chief) assessment that the Tirpitz had not sailed from her Norwegian port. Denning's assessment was based on ULTRA (communications intelligence) intercepts, and in fact, the Tirpitz remained in port. Nevertheless, the convoy dispersed on Pound's orders and became vulnerable to German air and submarine attacks. Twenty-three of the thirty-four merchant ships in the convoy were sunk in one of the worse disasters to befall any Allied convoy during World War II.

Patrick Beesly, who served in the OIC during World War II, offered the following analysis of why the fatal decision to scatter the convoy was made:

"Quite apart from age and health (Pound was 65 and would die from a brain tumor the next year), and despite his great experience as a staff officer, Pound did not, in my opinion, understand the intelligence scene. Although the OIC was only a few minutes' walk from his own office he very rarely visited it. He appreciated neither the strengths nor weaknesses of Special Intelligence: he required 'Yes' or 'No' answers to his question ('Can you assure me that Tirpitz is still in Altenfjord?') - something that the very best intelligence officers can seldom give. In all intelligence problems there must always be some element of uncertainty, always a last piece of the jigsaw puzzle which can only be filled in by guesswork. It may be inspired intuition, but it should always be based on thorough background knowledge of the enemy and his way of thinking. After three years of war it ought to have been obvious that Denning, one of the most brilliant intelligence officers of either world war, had this gift, but Pound could not bring himself to rely on so junior an officer's opinion. Events proved Denning right and Pound wrong. Senior officers, who have to take final responsibility, must not only fully understand the sources, methods, and extent of their intelligence organization, but also personally know their intelligence officers sufficiently well to assess their capabilities and to rely on their assessments or, if they are not satisfied, replace them."

SOURCE: Beesly, Patrick, Convoy PQ17, A Study of Intelligence and Decision Making, published in Intelligence and Military Operations, Michael I. Handel, ed., London, U.K.: Frank Cass & Company Limited, 1990, 292-322

Intentionally Blank

CHAPTER IV
INTELLIGENCE SUPPORT TO PLANNING, EXECUTING, AND ASSESSING JOINT OPERATIONS

"What is called 'foreknowledge' cannot be elicited from spirits, nor from gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation."

Sun Tzu *The Art of War, 400-320 BC*

1. A Systems Perspective of the Operational Environment

The planning, execution, and assessment of joint operations requires a systems perspective of the operational environment that connects strategic and operational objectives to tactical tasks by identifying desired and undesired effects. CCDRs plan joint operations by developing theater strategic objectives supported by measurable strategic and operational tasks. Joint operation planning uses measurable desired effects to relate higher-level objectives to component missions, tasks, and/or actions. The joint force J-2 plays a critical role in assisting the CCDR in the identification and development of measurable desired effects and assessment indicators based on a systems perspective of the operational environment. A full understanding of the operational environment typically will require cross-functional participation by other joint staff elements and collaboration with various intelligence organizations, OGAs, and nongovernmental centers of excellence.

a. **Holistic View.** The operational environment is a composite of the conditions, circumstance, and influences that affect the employment of capabilities and bear on the decisions of the commander. Understanding this environment requires a perspective broader than the adversary's military forces and other combat capabilities within the operational area. The planning, execution, and assessment of joint operations require a holistic view of all relevant systems that comprise the operational environment (See Figure IV-1).

(1) A "system" is a functionally, physically, and/or behaviorally related group of regularly interacting or interdependent elements that form a unified whole. Therefore, a systems perspective of the operational environment requires understanding a wide variety of systems, their interaction with each other, and how their relationships may change over time. Intelligence identifies and analyzes the adversary and other relevant systems and estimates how individual actions on one element of a system can affect other system components.

(2) As part of the JIPOE process, the joint force J-2 manages the analysis and development of products that provide a systems understanding of the adversary, and other relevant aspects of the operational environment. This analysis identifies a number of nodes — specific physical, functional, or behavioral entities within each system. Nodes can include people, facilities, individual systems, forces, information, and other components of the system. JIPOE analysts also identify links — the behavioral, physical, or functional relationship between nodes. The identification of links and nodes and subsequent analysis provide the foundation for developing a systems perspective of the operational environment. This analysis includes the identification

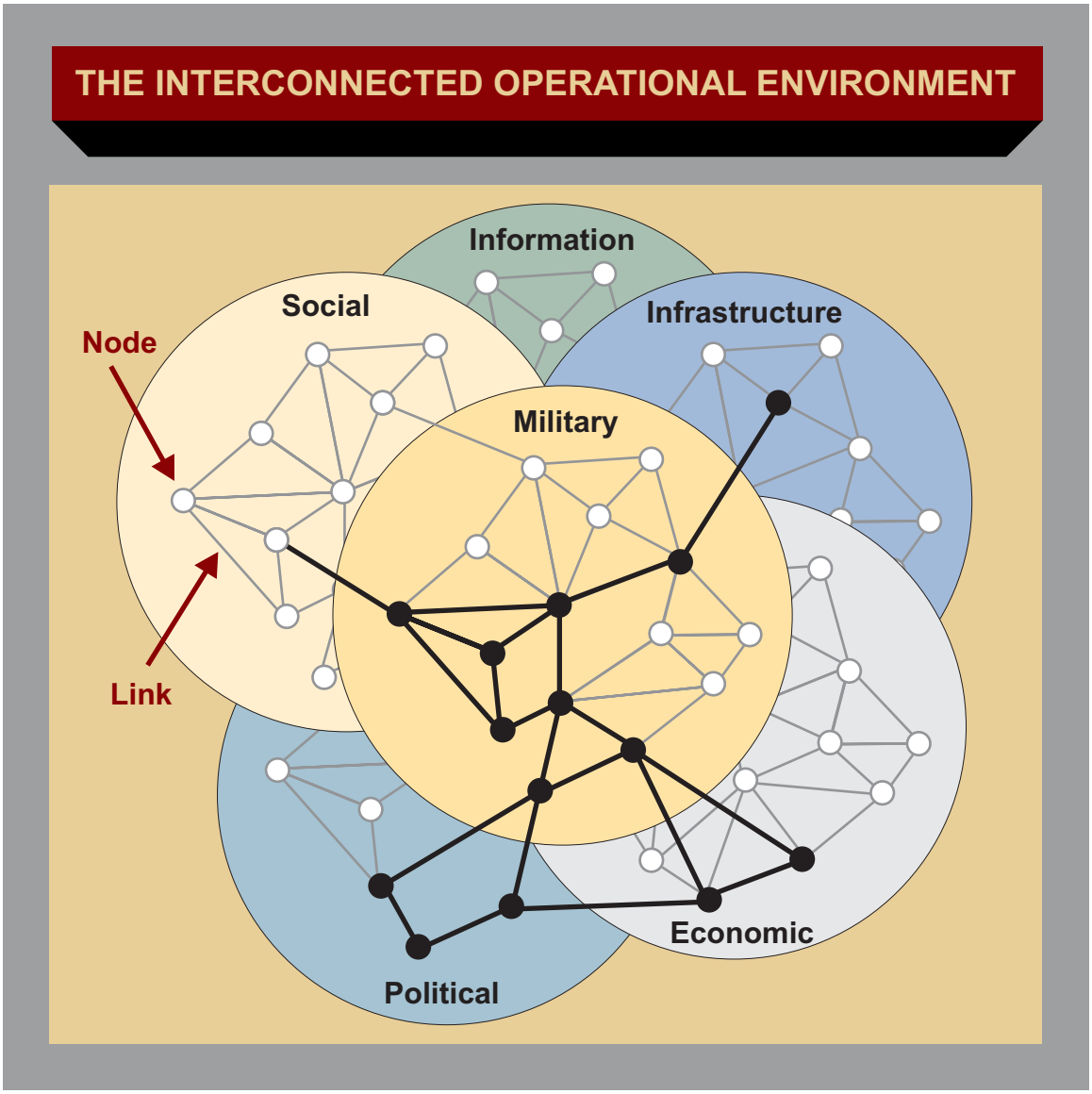


Figure IV-1. The Interconnected Operational Environment

of adversary COGs and decisive points for action to influence or change adversary system behavior and also provides the means by which intelligence personnel develop specific indicators of future adversary activity and COAs.

b. **Effects and Objectives.** An effect is the physical or behavioral state of a system that results from an action, a set of actions, or another effect. A desired effect could also be thought of as a condition that supports achieving an associated objective, while an undesired effect could inhibit progress toward an objective. A set of desired effects contributes to the conditions necessary to achieve an associated military objective. Desired or undesired effects can be created directly or indirectly. A direct effect is the proximate, first order consequence of an action, which usually is immediate and easily recognizable (such as the destruction of an early warning air defense radar site). An indirect effect is a delayed and/or displaced consequence associated with the

action that caused the direct effect (such as the degradation of the enemy's early warning air defense capability). Combined with a systems perspective, the identification of desired and undesired effects can help commanders and their staffs gain a common picture and shared understanding of the operational environment that promotes unified action. CCDRs plan joint operations by developing strategic objectives supported by measurable strategic and operational effects and assessment indicators. At the operational level, the JFC develops operational-level objectives supported by measurable operational effects and assessment indicators. Joint operation planning uses measurable effects to relate higher-level objectives to component missions, tasks, or actions.

SECTION A. PLANNING

2. General

Operation planning occurs in a networked, collaborative environment, which requires iterative dialogue among senior leaders, concurrent and parallel plan development, and collaboration across multiple planning levels. The focus is on developing plans that contain a variety of viable, embedded options (branches and sequels) for the President and Secretary of Defense to consider as the situation develops. This facilitates responsive plan development and modification, resulting in "living" plans (i.e., the systematic, on-demand, creation and revision of executable plans, with up-to-date options, as circumstances require). This type of adaptive planning also promotes greater involvement with other US agencies and multinational partners. Joint operation planning requires considerable sophistication in understanding an adversary's vulnerabilities, COGs, and ability to adapt to changing circumstances, in order to influence and shape events and provide options to planners and decision makers.

JP 5-0, Joint Operation Planning*, discusses joint operation planning in greater detail.*

a. Intelligence planning supports joint operation planning and results in three major products; a DIA produced dynamic threat assessment, a combatant command J-2 produced annex B (Intelligence), and a national intelligence support plan (NISP) produced by the DJIOC. Together the annex B and the NISP integrate and synchronize the intelligence capabilities of the combatant command and the DOD portion of the IC to answer the commander's focused intelligence needs to help achieve the JFC's objectives. (See Figure IV-2.)

b. The DJIOC, USSTRATCOM's JFCC-ISR, and combatant command JIOCs are the focal points for intelligence planning designed to synchronize the efforts of the DOD portion of the IC and to orchestrate the broader IC effort with the theater plan. Intelligence planning provides a comprehensive methodology for integrating intelligence into plans, and focusing IC capabilities on satisfying combatant command intelligence requirements. Intelligence planning should also include collection and production requirements related to critical infrastructure protection. The intelligence planning process is conducted in four phases that correspond to the four joint planning functions discussed in JP 5-0, *Joint Operation Planning*: strategic guidance, concept development, plan development, and plan assessment (See Figure IV-3).

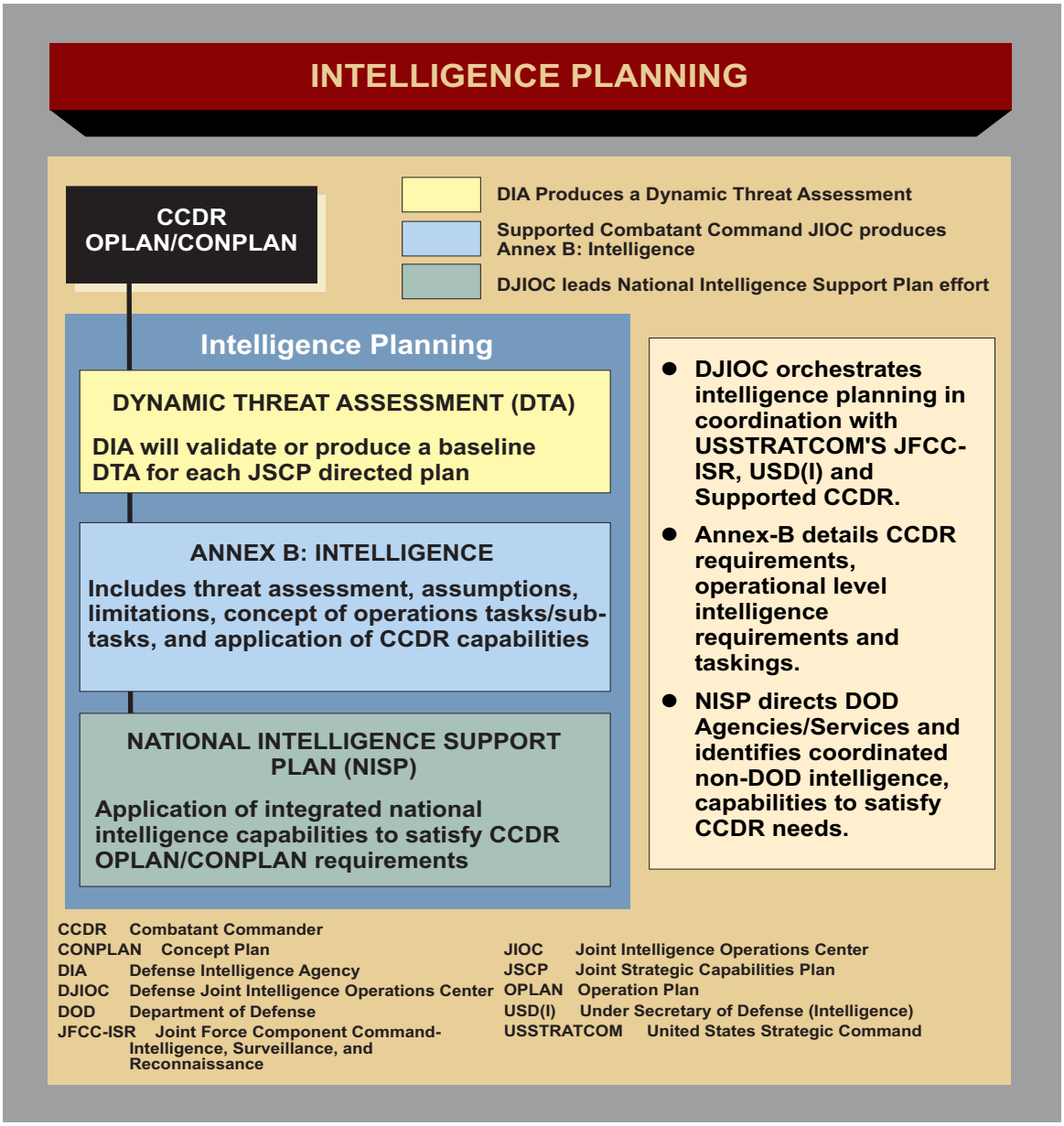


Figure IV-2. Intelligence Planning

3. Strategic Guidance

The Secretary of Defense and Chairman of the Joint Chiefs of Staff provide the combatant commands with intelligence planning guidance in the National Military Strategy, Contingency Planning Guidance (CPG), Joint Strategic Capabilities Plan (JSCP), and Intelligence Supplement to the JSCP. The JSCP directs CCDRs to use intelligence planning to integrate theater and national intelligence capabilities and synchronize their respective plan objectives for each OPLAN and CONPLAN. The Under Secretary of Defense for Policy (USD[P]) may provide additional

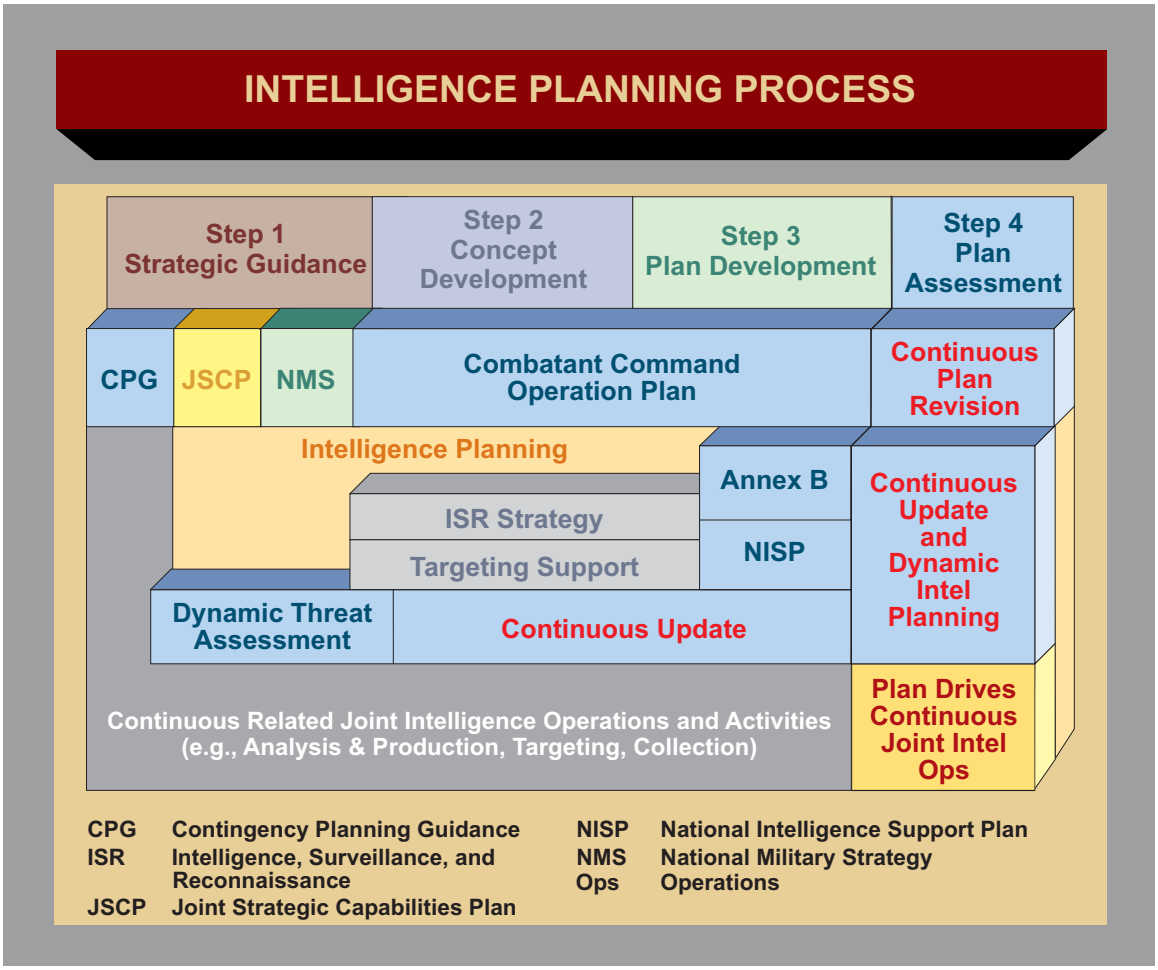


Figure IV-3. Intelligence Planning Process

amplifying guidance in the form of strategic guidance statements. The Chairman of the Joint Chiefs of Staff and CCDRs may also provide specific guidance.

a. During this phase, intelligence planners support a mission analysis in which strategic guidance documents are reviewed to determine all the assigned tasks, resources available, and an understanding of how the combatant command's mission objectives fit into the strategic purpose. This phase lays the groundwork for more detailed planning by developing an understanding of the mission and commander's intent; analyzing the impact of the operational environment on national intelligence capabilities; identifying specified and implied intelligence tasks; reviewing the availability of intelligence assets and capabilities; determining intelligence support limitations; proposing acceptable risk guidelines; determining facts and assumptions; and assessing the amount of time available for further planning. The combatant command staff, Joint Staff, USSTRATCOM's JFCC-ISR, DJIOC, and national ISR organizations assess the status and availability of their respective ISR assets and activities for inclusion in the NISP.

b. DIA develops and maintains a dynamic threat assessment (DTA) for each of the top priority plans identified in the CPG. DTAs are electronically updated intelligence assessments that detail the threat, capabilities, and intentions of adversaries. They are produced electronically

on a standardized template, coordinated throughout the IC and with the respective combatant command, disseminated not later than 30 days following the release of the CPG, and then updated continuously as relevant aspects of the operational environment change.

c. The combatant command J-2 begins preliminary information gathering in preparation to start development of annex B to the relevant OPLAN. The combatant command J-2 assesses the command's intelligence posture for the operation under consideration. Specifically, the combatant command J-2:

(1) Evaluates relevant databases, and identifies intelligence gaps and priorities.

(2) Evaluates status of information regarding target systems in the AOR.

(3) Assesses status of targeting information, including: comprehensiveness of target system analyses (TSAs); accuracy of target and NSLs; status of target folders, and other relevant target materials; and the need for relevant GI&S.

(4) Evaluates existing collection, exploitation, analytic, and production requirements. Due to the long lead time required to establish HUMINT collection capabilities, it is critical that coordinated HUMINT requirements be quantified as early as possible.

(5) In conjunction with the DJIOC, begins development of intelligence assumptions and identification of limitations (e.g., resource constraints) as mission analysis is completed within the planning process.

(6) Accomplishes (through the combatant command JIOC in coordination with the combatant command J-3, USSTRATCOM's JFCC-ISR, and force provider commanders) a preliminary assessment of global ISR assets and capabilities to prepare for development of an ISR strategy and annex B to the relevant OPLAN.

4. Concept Development

As part of concept development, intelligence planners participate in friendly COA development, analysis, comparison and selection. The JIPOE process identifies potential adversary COAs, and assesses which adversary COA is most likely and which COA is most dangerous to mission accomplishment. During COA analysis, each friendly COA is wargamed against the adversary COAs identified through the JIPOE process. Combatant command JIOCs play an integral role in the wargaming effort by among other things, accurately role playing the adversary and through the formation and use of red teams. The combatant command J-2 and JIOC analyze and evaluate the advantages and disadvantages of each friendly COA from an intelligence perspective and, in conjunction with other combatant command staff elements, provide a recommendation regarding the friendly COA with the highest probability of success. Following the CCDR's selection of a COA, the combatant command J-2 and JIOC produce a list of proposed PIRs, intelligence task list, ISR strategy, federated intelligence agreements, and functional intelligence support plans.

a. After the CCDR selects a COA and approves the proposed list of PIRs, the combatant command JIOC drafts a compilation (intelligence task list) of the specified and implied tasks required to satisfy the combatant command's intelligence needs. The intelligence task list is based on the CCDR's operational objectives, desired and undesired effects, tasks, and approved PIRs and associated EEIs, and includes subtasks that contribute to the satisfaction of individual task requirements. The draft intelligence task list is provided to the DJIOC for coordination with the DOD portion of the IC and is ultimately incorporated into the NISP in accordance with the DIAP. Through the DIAP, the responsibility for shared analysis and production to satisfy these tasks is assigned to the combat support agencies, Service intelligence centers, and the combatant command's production elements. The intelligence task list is also provided to DOD intelligence collection, processing, exploitation, and reporting organizations for incorporation in their respective functional support plans (See Figure IV-4).

b. Combat support agencies, national and Service intelligence support organizations, and international partners assess their current analysis and production capabilities, existing databases and intelligence holdings, and human resource availability to support plan development and execution.

c. USSTRATCOM's JFCC-ISR develops a global ISR strategy that is used by the DJIOC and the combatant command JIOCs in the formulation of their ISR strategies. The JIOC, in coordination with the DJIOC and USSTRATCOM's JFCC-ISR, develops a combatant command ISR strategy based on the CCDR's objectives, guidance, and intent. This ISR strategy identifies the ISR goals to be achieved during each phase of the operation and provides guidance for the development of the command's ISR architecture.

d. The JIOC assesses the capabilities of the combatant command's ISR and analytic assets to fulfill the command's intelligence needs (as expressed in the intelligence task list). Gaps between capabilities and requirements are identified as shortfalls and provide the basis for requesting augmentation and/or the establishment of federated intelligence partnerships with other organizations. DOD IC organizations may also begin drafting functional support plans in areas such as all-source analysis and production, linguistics and translation services, document and materiel exploitation, CI, HUMINT, GEOINT, MASINT, and SIGINT operations.

5. Plan Development

During plan development, the CCDR and staff, in collaboration with subordinate and supporting components and organizations, expand the approved COA into a detailed joint OPLAN by first developing an executable CONOPS. The CCDR's CONOPS describes how the actions of the joint force components and supporting organizations will be integrated, synchronized, and phased to accomplish the mission, including potential branches and sequels.

a. As part of plan development, the combatant command J-2 develops a concept of intelligence operations that supports the CCDR's CONOPS. The concept of intelligence operations provides broad guidance regarding the intelligence mission, assumptions, intent, limitations, and priority of effort for each phase of the operation.

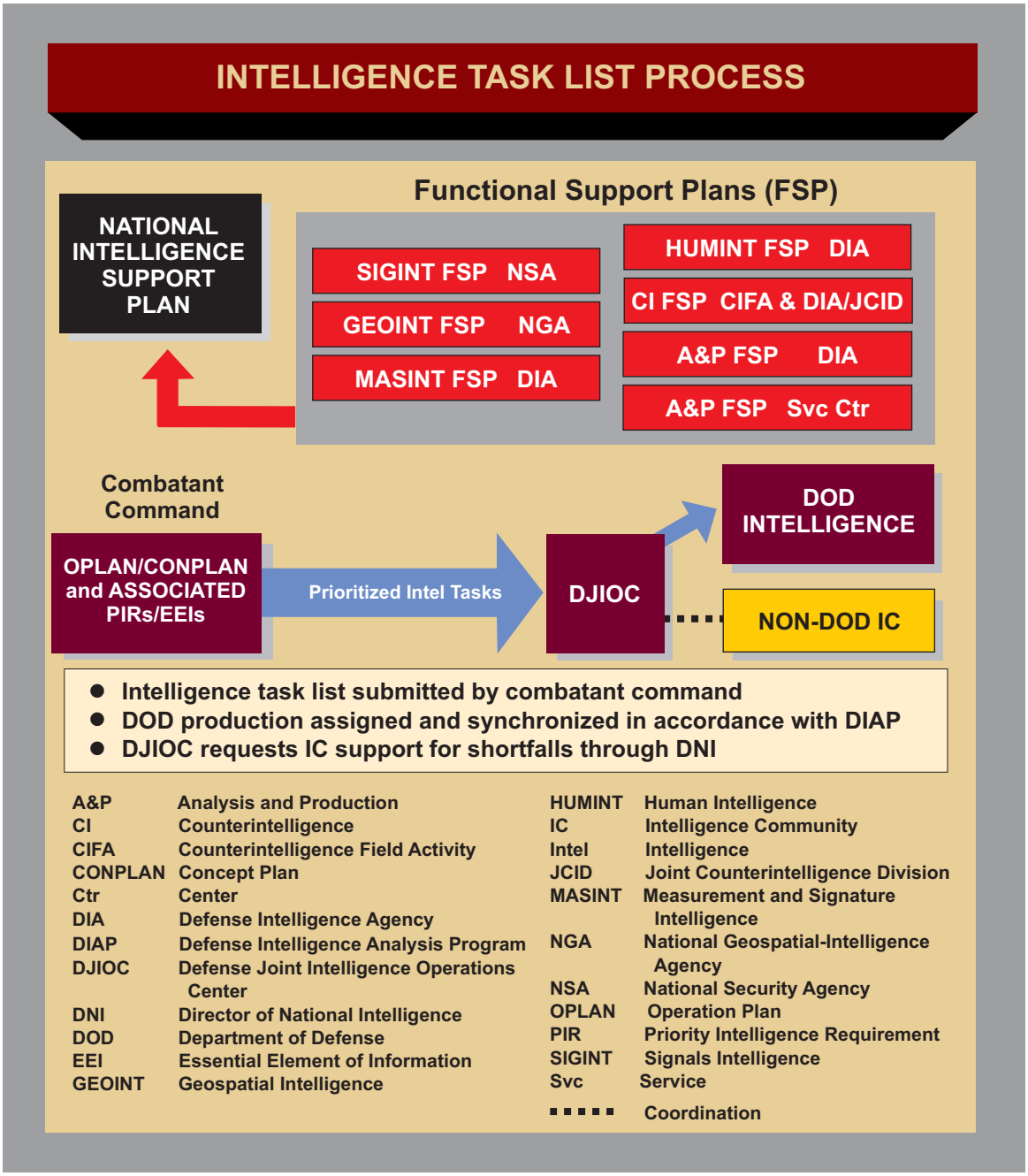


Figure IV-4. Intelligence Task List Process

b. The JIOC identifies the minimum resource requirements necessary to support the OPLAN and develops mitigation strategies to reduce the risk associated with any shortfalls in collection, analysis, and production capabilities. Any shortfalls in the combatant command's intelligence capabilities, or alternatively any overlap with the intelligence capabilities in the NISP, are addressed with the DJIOC. The DJIOC works with the JIOC to develop the most efficient and effective intelligence support plan possible by avoiding duplication and focusing on combatant command requirements.

c. As part of plan development, the JIOC drafts annex B (Intelligence) to the OPLAN and submits it to the DJIOC for coordination with the DOD portion of the IC. Annex B (Intelligence) is also coordinated through the joint planning and execution community as part of the plan approval process. Annex B (Intelligence) is based on and incorporates the intelligence support planning products completed earlier as part of strategic guidance and concept development (i.e., the concept of intelligence operations, ISR strategy and CONOPS, intelligence task list, identification of capability shortfalls and mitigation strategies, DTA, and intelligence estimate).

d. A NISP is completed for each of the top priority plans during plan development. It defines the collection, analysis, and production support roles and responsibilities of the DOD portion of the IC within the combatant command's AOR to ensure fully integrated and synchronized intelligence support to the OPLAN. As part of NISP development, the DJIOC, through USD(I), tasks appropriate organizations within the DOD IC to develop functional support plans that specify the type of support they will provide to the OPLAN. The DJIOC sends the final NISP, functional intelligence support plans, federated intelligence agreements, and intelligence task list to the CCDR for approval. After combatant command approval, the package is staffed with all participating organizations and the Joint Staff, provided in turn to the Joint Staff J-2, Chairman of the Joint Chiefs of Staff, USD(P), and USD(I) for concurrence, and after final concurrence is delivered to the Chairman of the Joint Chiefs of Staff for signature. This staffing occurs either after or in conjunction with the staffing of the supported OPLAN.

6. Plan Assessment (Refine, Adapt, Terminate, Execute)

During this function, the CCDR refines the complete plan while supporting and subordinate commanders, Services, and supporting agencies complete their plans for review and approval. In general, the CCDR will, when required, submit the plans for the Secretary of Defense's approval. All commanders continue to develop and analyze branches and sequels as required. The CCDR, the Joint Staff, and subordinate commanders continue to evaluate the situation for any changes that would trigger plan refinement, adaptation, termination, or execution. This includes monitoring current readiness and availability status to assess sourcing impacts and to develop sourcing COAs should the plan be considered for near-term implementation. The combatant command JIOC and the DJIOC monitor and maintain annex B (Intelligence) to the OPLAN, the NISP, and the intelligence task list, incorporating changes as necessary. As part of plan refinement, updates are posted to the DTA as changes occur in the operational environment. During the plan assessment in progress review, the CCDR will brief the Secretary of Defense regarding any identified requirements to adapt, terminate, or execute an OPLAN.

For more detailed information on the intelligence aspects of joint operation planning, to include formats for intelligence support planning products, see JP 2-01, Joint and National Intelligence Support to Military Operations.

FUNCTION OF INTELLIGENCE ESTIMATES

"The estimate, in its entirety, is a presentation of possibilities:

• the forces available to the other side that may interfere and disrupt the military operation;
• the available weapons systems and their operational characteristics; and
• the possible timetable of intervention.

This is clearly not an attempt to predict the course of events. On the contrary, it can be stated with near certainty that these 'possible courses of action' available to the enemy will never materialize, the most drastic, severe, and perilous possibilities having been deliberately chosen for presentation. Furthermore, what really happens depends, of course, on the decisions made by the other side, their timing, their rate of implementation, the combat readiness of their forces and their speed of action. The true test of intelligence does not lie in whether these possibilities actually occur, but in whether forces of whose existence intelligence was unaware come into play, or if their speed of intervention exceeds the intelligence forecast.
For instance, before the 'Entebbe Operation' (July 1976), intelligence pointed out the existence of Ugandan MIG fighters at the Entebbe airport and the possibility (even though of low probability) that they could be used to shoot down the fleet of Israeli Hercules transports during the flight north after the rescue. Israel's government, basing its decision on these data and the estimate, ordered the destruction of the MIGs on the ground to ensure the safe flight of the task force and the hostages."

SOURCE: Major General Shlomo Gazit
Chief, Israeli Military Intelligence, 1974-1979

SECTION B. EXECUTION

7. General

Execution begins when the President decides to use a military option to resolve a crisis. Only the President or Secretary of Defense can authorize the Chairman of the Joint Chiefs of Staff to issue an execute order (EXORD). The EXORD directs the supported commander to initiate military operations, defines the time to initiate operations, and conveys guidance not provided earlier. The Chairman of the Joint Chiefs of Staff monitors the deployment and employment of forces, acts to resolve shortfalls, and directs action needed to ensure successful completion of military operations. Execution continues until the operation is terminated or the mission is accomplished or revised. Execution consists of mobilization, deployment, employment, sustainment, redeployment, and demobilization activities. Intelligence support is crucial to all aspects of execution. For example, CI support to force protection and operations security (OPSEC) is particularly critical during mobilization and deployment; intelligence assessments regarding the current status of foreign transportation infrastructure (airfields, seaports, etc.) are vital to the

success of deployment and redeployment operations; MEDINT enables decision makers to devise protection measures to mitigate combat-related battle injuries and disease and nonbattle injuries during deployment, employment, and redeployment; and intelligence analyses of threats to air, land, and sea lines of communications (LOCs) are critical to sustainment operations. Immediate, precise, and persistent intelligence support to force employment is a particularly important prerequisite for military success throughout all phases of a joint operation (i.e., shaping, deterrence, seizing the initiative, dominance, stabilization, and enabling civil authority) regardless of how the battle evolves. JIOCs must be familiar with specific phasing arrangements of each command operation plan because the phasing may differ for specific types of operations. See Figure IV-5. During execution, intelligence must stay at least one step ahead of operations and not only support the current phase of the operation, but also simultaneously lay the informational groundwork required for subsequent phases. Execution of joint operations requires optimizing the use of limited ISR assets and maximizing the efficiency of intelligence production resources and is the ultimate test of the efficacy of intelligence support planning.

JP 4-05, Joint Mobilization Planning, *discusses joint mobilization and demobilization in greater detail. JP 3-35,* Joint Deployment and Redeployment Operations, *discusses joint deployment and redeployment execution in greater detail. JP 3-0,* Joint Operations, *and JP 5-0,* Joint Operation Planning, *discuss joint employment in greater detail. JP 4-0,* Logistic Support of Joint Operations, *discusses joint sustainment operations in greater detail.*

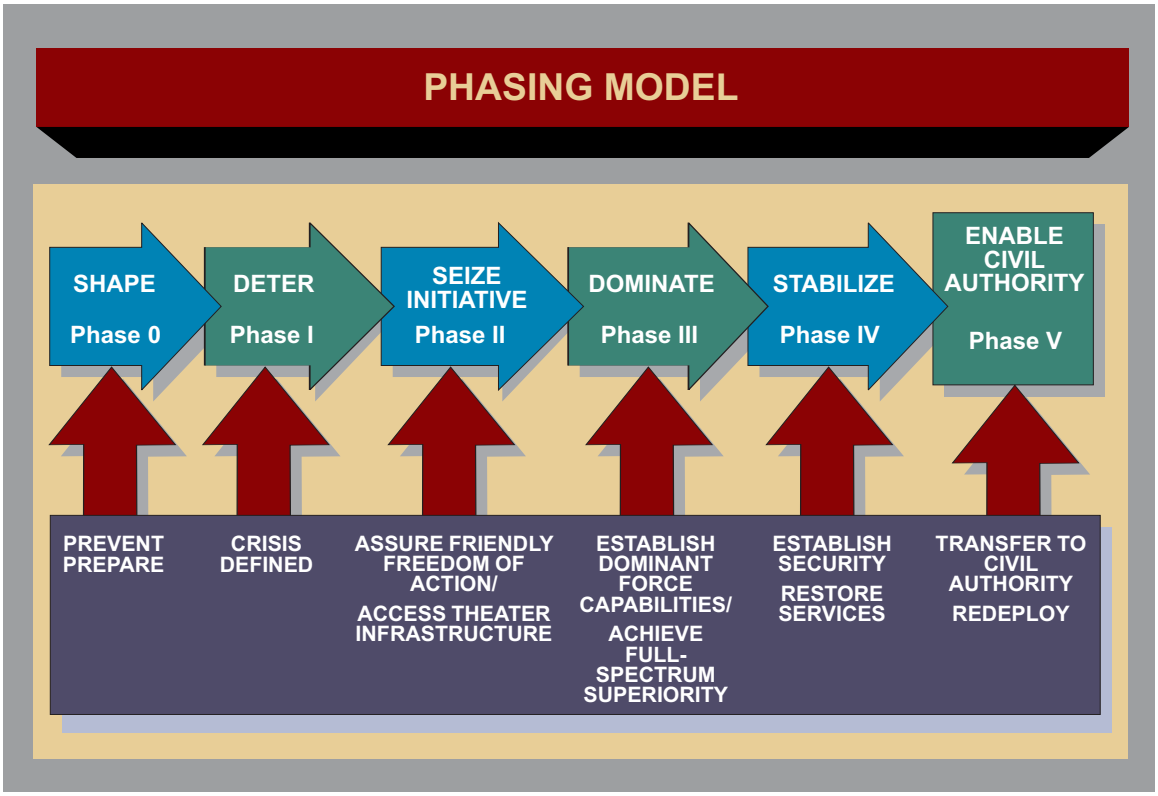


Figure IV-5. Phasing Model

8. Intelligence Support During the Shaping Phase

JFCs are able to take actions before committing forces to assist in determining the shape and character of potential future operations. In many cases, these actions enhance bonds between future coalition partners, increase understanding of the region, help ensure access when required, strengthen future multinational operations, and prevent crises from developing. Intelligence activities conducted during the shaping phase lay the groundwork for intelligence operations in all subsequent phases of the operation.

a. Intelligence liaison with host nations and the establishment of multilateral intelligence sharing arrangements with multinational partners are critical aspects of the shaping phase. Whenever possible, and in coordination with the responsible DNI representative, JFCs should engage host nations and coalition members by ensuring the participation of US personnel in mutual intelligence training, temporary exchanges of intelligence personnel, federated intelligence arrangements, and the integration and exercise of ISR support architectures. National intelligence cells should be formed as early as possible and a multinational intelligence center should be established to coordinate their activities. Foreign disclosure procedures should be put in place and exercised to the maximum extent feasible throughout this phase.

b. The combatant command JIOC should initiate a system-oriented JIPOE effort that will provide the basis for intelligence operations in all subsequent phases. The JIPOE effort during the shaping phase should focus on initial target development resulting in target lists and target material production, identification of adversary COGs, vulnerabilities and susceptibilities to information operations, critical key nodes, LOCs, and potential adversary COAs to deny friendly access to bases and lodgment areas. Whenever possible, host nation and coalition participation in the JIPOE effort should be encouraged.

c. Theater intelligence collection capabilities should be optimized by integrating (to the maximum extent feasible) the various intelligence capabilities of the combatant command, host nation, and coalition partners. Many potential multinational partners have niche capabilities that may prove invaluable to successful intelligence operations. For example, due to the long lead time required to establish HUMINT collection capabilities, it is important that coordinated HUMINT operations be initiated in the operational area as early as possible.

d. Intelligence support to IO is critical during the shape phase. An analysis and assessment of the adversary leadership structure and decision-making process must be performed as early as possible to determine what actions may serve as effective deterrents. Likewise, intelligence support to psychological operations (PSYOP) units tasked with determining potential foreign target audiences should be assessed as early as possible to focus the PSYOP effort and provide the lead time necessary for providing timely PSYOP product development, design, and approval.

e. Intelligence support, particularly human factors analysis, is essential to maximize the effectiveness of civil-military operations (CMO). An analysis and assessment of the civil dimension in targeted countries, that identifies civil society key influences, individuals, organizations, structures, and areas must be performed as early as possible to determine what

civil engagement actions may serve as effective points of influence. Likewise, intelligence support to CMO should be assessed as early as possible to focus the CMO effort and provide the lead-time necessary to provide timely planning, resource allocation, and mission execution.

9. Intelligence Support During the Deterrence Phase

Before the initiation of hostilities, the JFC must gain a clear understanding of the national and military strategic objectives; desired and undesired effects; actions likely to create those effects; COGs and decisive points; and required joint, multinational, and nonmilitary capabilities matched to available forces. The joint force J-2 assists the JFC in visualizing and integrating relevant considerations regarding the operational environment into a plan that will lead to achievement of the objectives and accomplishment of the mission. It is therefore imperative that the JIPOE effort (initiated during the shaping phase) provide the JFC with an understanding of the operational environment at the outset of the deterrence phase.

a. Intelligence support to IO is also critical during the deterrence phase. The adversary leadership structure and decision-making process must be continuously monitored and reassessed to determine what actions may serve as effective deterrents. The receptiveness of foreign target audiences to specific PSYOP programs should also be continuously assessed to support the overall IO effort.

b. During the deterrence phase, the ongoing JIPOE effort is accelerated to focus on monitoring the current situation while simultaneously assessing adversary capabilities to affect subsequent phases of the operation. JIPOE analysts support I&W by looking for specific indications of imminent adversary activity that may require an immediate response or an acceleration of friendly decision-making processes. JIPOE efforts also concentrate on confirming adversary COGs and support the continuous refinement of estimates of adversary capabilities, dispositions, intentions, and probable COAs within the context of the current situation. At the same time however, JIPOE analysts must look ahead and prepare threat assessments to support future operations planned for the seizing the initiative, dominance, and stabilization phases.

c. During the deterrence phase, COA development is dependent on detailed TSAs. TSAs identify and detail the functional components within the operational environment which may be influenced to gain a desired effect supporting the commander's objectives. As COAs are developed, targeteers nominate targets to either the JTL or RTL and place protected objects or entities on the NSL.

d. GEOINT support is critical during the deterrence phase. It is essential that any maps, charts, imagery products, and support data — to include datum and coordinate systems — to be used in a joint operation be fully coordinated with joint force components as well as with the Joint Staff, OSD, and NGA. The joint force J-2 works with the JFC staff and component command staffs to identify requirements for updated GEOINT products and submits these requirements through the NGA liaison team.

More detailed guidance regarding GEOINT procedures is contained in JP 2-03, Geospatial Intelligence Support to Joint Operations.

e. Selected intelligence operations may also serve as a flexible deterrent option — a preplanned, deterrence-oriented action carefully tailored to bring an issue to early resolution without armed conflict. For example, the deployment of additional ISR resources in the operational area not only increases intelligence collection capabilities and provides early warning, but may also demonstrate US resolve without precipitating an armed response from the adversary. Likewise, intelligence sharing arrangements, conferences, training, and exercises with the host nation may serve to reinforce US commitment to the host nation thereby deterring undesired adversary actions.

f. Intelligence may also support actions designed to isolate an adversary by identifying their potential allies and sanctuaries. Intelligence may also identify and assess the vulnerability to interdiction of the adversary's sources of support, to include intelligence support from other nations, international sympathizers, and commercial space surveillance assets. Neutralization of selected elements of the adversary's intelligence collection capabilities is particularly important and serves to reinforce their isolation, facilitates their susceptibility to IO, and at the same time helps protect friendly forces from detection.

g. Intelligence support to CMO during the deterrence phase can amplify operations to isolate the adversary. An analysis and assessment of the civil dimension of potential allies or supporters of the adversary may determine what civil engagement actions may serve as effective points of influence. Additionally, analysis of the civil dimension of friendly countries, especially in countries where US forces will require access for subsequent phases, will suggest appropriate civil engagement targets for CMO that may reduce enemy freedom of action while enhancing that of the US operational commander.

10. Intelligence Support During the Seizing the Initiative Phase

As operations commence, the JFC needs to exploit friendly asymmetric advantages and capabilities to shock, demoralize, and disrupt the enemy immediately. The JFC seeks decisive advantage through the use of all available elements of combat power to seize and maintain the initiative, deny the enemy the opportunity to achieve its objectives, and generate in the enemy a sense of inevitable failure and defeat. Additionally, the JFC coordinates with the appropriate interagency representatives through a joint interagency task force, joint interagency coordination group, or individually to facilitate coherent use of all instruments of national power in achieving national strategic objectives. JFCs and their J-2s should be on continuous guard against any enemy capability which may impede friendly force deployment from bases to ports of embarkation to lodgment areas.

a. The JFC's target intelligence element is particularly active in this phase. It is responsible for gathering target nominations; vetting targets; matching target vulnerabilities with appropriate agents (weaponeering); coordinating with operations personnel to prioritize the targets for attack;

monitoring the ongoing operations for changes to the plan; conducting assessment; and providing input for further strategy and planning.

b. Intelligence support to IO and OPSEC is particularly important during this phase. CI supports force protection during deployment from home bases to lodgment areas. HUMINT, SIGINT, and OSINT sources may detect indications of enemy demoralization and thereby provide valuable insight into the PSYOP success or failure. The combatant command JIOC red team may prove extremely valuable to friendly deception planning efforts. The JIOC red team may use a "reverse JIPOE" process to analyze the friendly force from the adversary's perspective, identify potential indicators of friendly COAs, and provide insight into the possible times and locations of the adversary's intelligence collection plan. This insight assists deception planners in determining the best times and locations to plant deceptive information designed to mislead adversary intelligence analysts.

JIPOE support to deception planning is discussed in greater detail in JP 2-01.3, Joint Intelligence Preparation of the Operational Environment (JIPOE).

c. Real-time, persistent surveillance and dynamic ISR collection management are important throughout the execution of joint operations, but are particularly critical during the seizing the initiative and dominance phases. Adversary force deployments must be tracked with a level of persistence and accuracy sufficient to support retargeting and precision engagement. An ISR strategy that fully integrates and optimizes the use of all available US, coalition, and host-nation ISR assets is essential to persistent surveillance. Furthermore, the combatant command JIOC facilitates ISR collection management through ISR visualization — the continuous real-time monitoring of the status, location, and reporting of ISR platforms and sensors. ISR visualization provides real-time cross cueing and provides a basis for re-tasking and time-sensitive decision-making.

Persistent surveillance and ISR visualization are discussed in greater detail in JP 2-01, Joint and National Intelligence Support to Military Operations.

11. Intelligence Support During the Dominance Phase

During the dominance phase, JFCs conduct sustained combat operations by simultaneously employing conventional, SOF, and IO capabilities throughout the breadth and depth of the operational area. CMO is executed to preclude civilian interference in attainment of operational objectives or to remove civilians from operational areas. Operations may be linear (i.e., combat power is directed toward the enemy in concert with adjacent units) or nonlinear (i.e., forces orient on objectives without geographic reference to adjacent forces). Some missions and operations (i.e., strategic attack, interdiction, and IO) are executed concurrently with other combat operations to deny the enemy sanctuary, freedom of action, or informational advantage. JFCs may design operations to cause the enemy to concentrate their forces, thereby facilitating their attack by friendly forces, or operations may be designed to prevent the enemy from concentrating their forces, thereby facilitating their isolation and defeat in detail.

The use of long endurance, unmanned aerial vehicles, such as the MQ-1 Predator, greatly facilitates real-time, persistent surveillance.

a. Intelligence must be equally prepared to support linear and nonlinear operations. Nonlinear operations are particularly challenging due to their emphasis on simultaneous operations along multiple lines of operations. The complexity of nonlinear operations places a premium on a continuous flow of accurate and timely intelligence to help protect individual forces. This flow of intelligence supports precise targeting, mobility advantages, and freedom of action and is enabled by persistent surveillance, dynamic ISR management, and a common intelligence picture (the intelligence portion of the COP).

b. An enemy's use, or threatened use, of weapons of mass destruction (WMD) can quickly change the character of an operation or campaign, threaten the cohesion of alliances and coalitions, and cause large-scale shifts in strategic and operational objectives, phases, and COAs. J-2s provide JFCs and component commanders with assessments of an enemy's capability, willingness and intent to employ WMD. These assessments should identify known and suspected locations of enemy WMD stockpiles and delivery systems, anticipate the conditions under which the enemy is most likely to use WMD, and analyze the effects on the operational environment of WMD use.

c. Intelligence must not only support operations during the dominance phase, but also anticipate and address the information requirements for the subsequent stabilization phase. For example, intelligence must be prepared to assist the JFC in determining how to fill the power vacuum after the conclusion of sustained combat operations. In order to set the groundwork for stability, security, transition, and reconstruction operations, the JFC will require detailed intelligence regarding the status of key infrastructure, enemy government organizations and personnel, and anticipated humanitarian needs.

12. Intelligence Support During the Stabilization Phase

Stabilization typically begins with significant military involvement to include some combat, then moves increasingly toward enabling civil authority as the threat wanes and civil infrastructures are reestablished. As progress is made, military forces increase their focus on supporting the efforts of host nation authorities, OGAs, IGOs, and/or NGOs.

a. During the stabilization phase, intelligence collection and analysis should transition from supporting combat operations to focus on actual or potential threats to the joint force (e.g., insurgent groups, criminal elements, terrorist cells). Particular attention should be paid to identifying and assessing the leaders of groups posing potential threats to civil authority and reconstruction efforts. Intelligence should also identify critical infrastructure and analyze its vulnerability to disruption by elements hostile to stabilization efforts. Critical infrastructure vulnerability analysis may require coordination and assistance from OGAs.

b. CI support to force protection is critical during the stabilization phase. Host nation authorities, OGAs, IGOs, and NGOs working closely with US forces may pass information (knowingly or unknowingly) to hostile elements that enables them to interfere with stability operations. Likewise, members of the local populace may have access to US bases in order to provide essential services and friendly forces may recruit former regime officials to participate in stabilization efforts. CI elements help screen and vet foreign personnel and investigate instances of compromised sensitive information.

c. PSYOP are a critical aspect of stabilization. Intelligence helps assess the relative effectiveness of PSYOP in changing the behavior of the local populace to support civil authorities and reconstruction efforts. Additionally, DIA's human factors assessments of the foreign leadership's susceptibility to PSYOP can assist commanders in determining the best COAs to achieve stabilization.

13. Intelligence Support During the Enabling Civil Authority Phase

This phase is characterized by the establishment of a legitimate civil authority that is enabled to manage the situation without further outside military assistance. In many cases, the United States will transfer responsibility for the political and military affairs of the host nation to another authority. The joint operation normally is terminated when the stated military strategic and/or operational objectives have been met and redeployment of the joint force is accomplished.

a. In some situations, intelligence support may remain in place after termination of the joint operation in order to support the civil authority and/or to continue to monitor the situation. As in the deterrence phase, intelligence resources may serve as a valuable tool for demonstrating US resolve and commitment to the host nation. To facilitate this critical role in establishing friendly relations with the new civil authority, intelligence sharing agreements should be promulgated as soon as practicable.

b. Before the operation is terminated, it is important that all intelligence lessons learned are recorded in appropriate databases and are captured in joint doctrine. Likewise, the joint force J-2 should ensure that all JIPOE products, intelligence assessments, collection plans, and J-2X source registries are appropriately archived. This material may prove valuable to operation planning in the event US forces are directed to redeploy to the area.

SECTION C. ASSESSMENT

14. General

Continuous and timely assessments are essential to measure progress of the joint force toward mission accomplishment. Commanders continuously assess the operational environment and the progress of operations, and then compare them to their initial vision and intent. Commanders and their staffs determine relevant assessment actions and measures during planning. They consider assessment measures as early as mission analysis, and include assessment measures and related guidance in commander and staff estimates. They use assessment considerations to help guide operational design in order to improve the sequence and type of actions along lines of operation. During execution, they continually monitor progress toward accomplishing tasks, creating effects, and achieving objectives. Assessment actions and measures help commanders adjust operations and resources as required, determine when to execute branches and sequels, and make other critical decisions to ensure current and future operations remain aligned with the mission and desired end state**.** Assessment occurs at all levels and across the entire range of military operations. Strategic and operational-level assessment efforts concentrate on broader tasks, effects, objectives, and progress toward the end state, while tactical-level assessment focuses on task accomplishment. Even in operations that do not include combat, assessment of progress is just as important and can be more complex than traditional combat assessment. **Normally, the joint force J-2 assists the J-3 in coordinating assessment activities.**

a. The joint force J-2, through the combatant command JIOC, helps the commander by assessing adversary capabilities, vulnerabilities, and intentions, and monitoring the numerous aspects of the operational environment that can influence the outcome of operations. The J- 2 also helps the commander and staff decide what aspects of the operational environment to measure and how to measure them to determine progress toward accomplishing a task, creating an effect, or achieving an objective. Intelligence personnel use the JIPOE process to provide JFCs and their staffs with a detailed understanding of the adversary and other aspects of the operational environment.

b. Intelligence personnel in the combatant command JIOC provide objective assessments to planners that gauge the overall impact of military operations against adversary forces as well as provide an assessment of likely adversary reactions and counteractions. The CCDR and subordinate JFCs should establish an assessment management system that leverages and synergizes the expertise of operations and intelligence staffs.

15. Assessment Process

The assessment process uses measures of performance (MOPs) to evaluate task performance at all levels of war, and measures of effectiveness (MOEs) to determine progress of operations toward achieving objectives. MOPs are used to measure task accomplishment, and answer the question "was the action taken, were the tasks completed to standard" to produce the desired effect. MOEs are used at the strategic, operational, and tactical-level, by J-2s to assess changes in adversary behavior, capabilities, or the operational environment. MOEs help answer questions like: "are we doing the right things, are our actions producing the desired effects, or are alternative actions required?" Well-devised measures can help the commanders and staffs understand the causal relationship between specific tasks and desired effects.

a. Both MOPs and MOEs can be quantitative or qualitative in nature, but meaningful quantitative measures are preferred because they are less susceptible to subjective interpretation. MOEs are based on observable and measurable indicators. Indicators provide evidence that a certain condition exists or certain results have or have not been attained, and enable decisionmakers to assess progress towards the achievement of the objective. Several indicators may make up an MOE, just like several MOEs may assist in measuring progress toward achievement of an objective.

b. Many indicators are developed through the JIPOE process and are observable through GEOINT, SIGINT, HUMINT, MASINT, OSINT, and friendly force mission reports (MISREPs), as well as by other means. MISREPs are used in most aspects of combat assessment, since they typically offer specific, quantitative data or a direct observation of an event to determine accomplishment of tactical tasks. (See Figure IV-6)

The assessment process is explained in greater detail in JP 3-60, Joint Targeting, *JP 3-0*, Joint Operations, *and JP 5-0*, Joint Operation Planning.

16. Strategic and Operational-Level Assessment (Effects Assessment)

Strategic and operational-level assessment efforts concentrate on broad tasks, effects, objectives, and progress toward the military end state. Continuous assessment helps the JFC and joint force component commanders determine if the joint force is "doing the right things" to achieve objectives, not just "doing things right." The use of a red team to critically examine the MOE from the perspective of the adversary will help ensure the JFC is measuring the "important things". The JFC also can use MOEs to determine progress toward success in those operations for which tactical-level combat assessment ways, means, and measures do not apply. Intelligence analysts use the JIPOE process to assist in the identification of desired and undesired effects and the development of related MOEs by analyzing adversary COAs, COGs, key nodes and links, and other significant characteristics of the operational environment as they relate to the friendly mission, end state and objectives. The JIPOE process is particularly valuable in identifying and developing indicators (which may be used as the basis for MOEs) to monitor changes in adversary system behavior, capabilities, or the operational environment. JIPOE support to assessment encompasses all aspects (political, military, economic, social, informational, and infrastructural) of the operational environment. This holistic perspective is facilitated by a collaborative

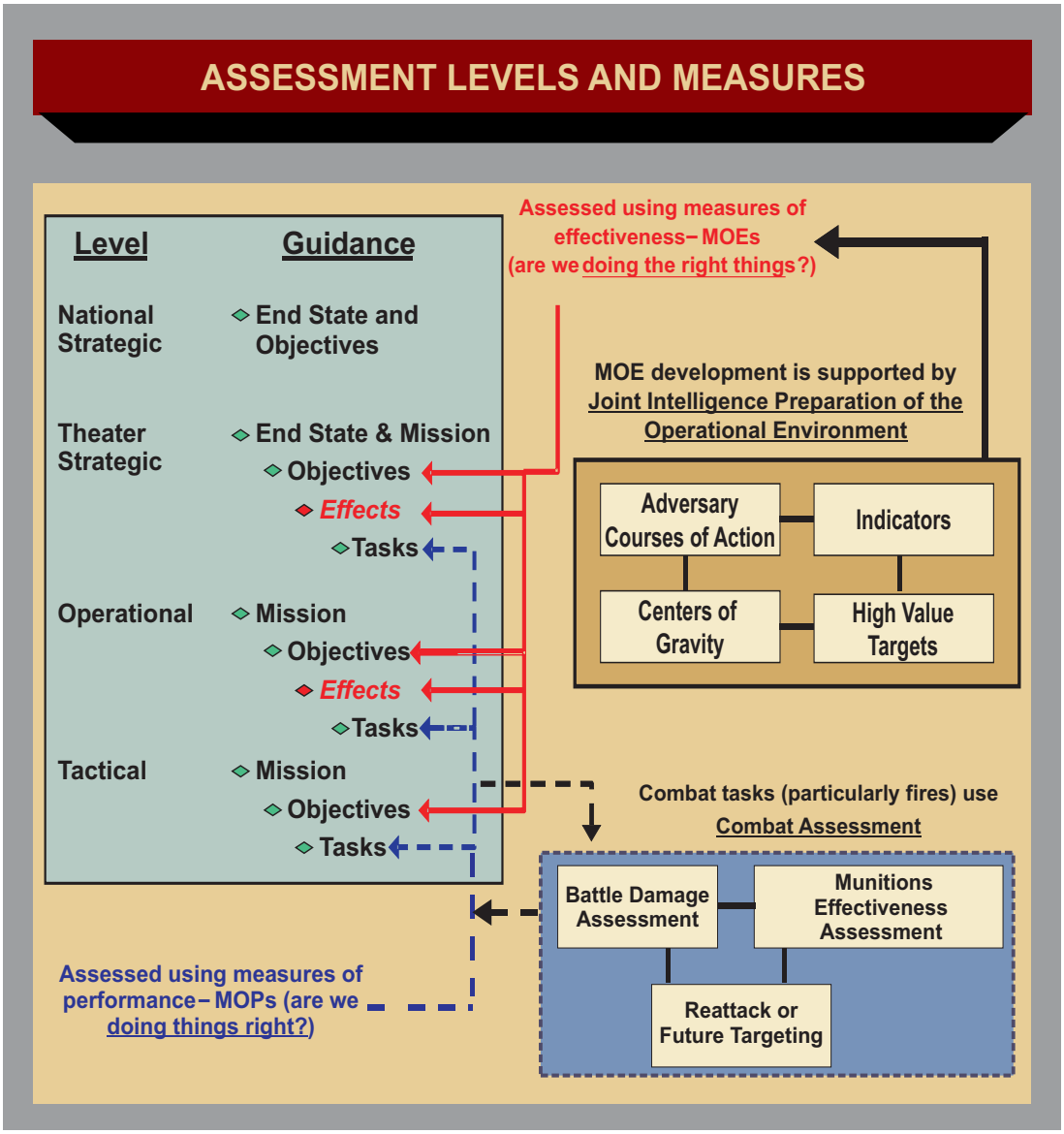


Figure IV-6. Assessment Levels and Measures

information environment that leverages the joint force's JIPOE effort with the expertise resident throughout the interagency community, multinational partners, and other appropriate centers of excellence.

a. A systems-oriented JIPOE effort is crucial to the identification of adversary COGs, key nodes and links. A COG can be viewed as a source of power that provides moral or physical strength, freedom of action, or will to act. COG analysis requires knowledge of an adversary's physical and psychological strengths and weaknesses and how the adversary organizes, fights, and makes decisions. Human factors analysis of the adversary's leadership is critical to assessing its strengths and weaknesses and how decisions are made. The JIPOE analyst must also have a detailed understanding of how each aspect of the operational environment links to the others and how various permutations of such links and nodes may combine to form COGs. For example, Figure IV-7 shows strategic and operational COGs, each consisting of a set of nodes and links. The operational

COG resides in the military system, while the strategic COG focuses in the political system but overlaps with the operational COG.

b. JIPOE analysts should assess the importance and vulnerabilities of all operationally relevant nodes and all primary and alternative links to those nodes. This is accomplished by combining an analysis of the constraints imposed by the operational environment with an evaluation of the adversary's preferred method or means of conducting a specific type of operation or activity (e.g., attack, defense, proliferation, WMD production, financing terrorist cells). The resulting product may take the form of a three dimensional situation template or model that identifies all the nodes and links associated with individual COAs or options available to the adversary within a specific category of activity. For example, analysis of an adversary's nuclear program may require separate situation templates to depict the links

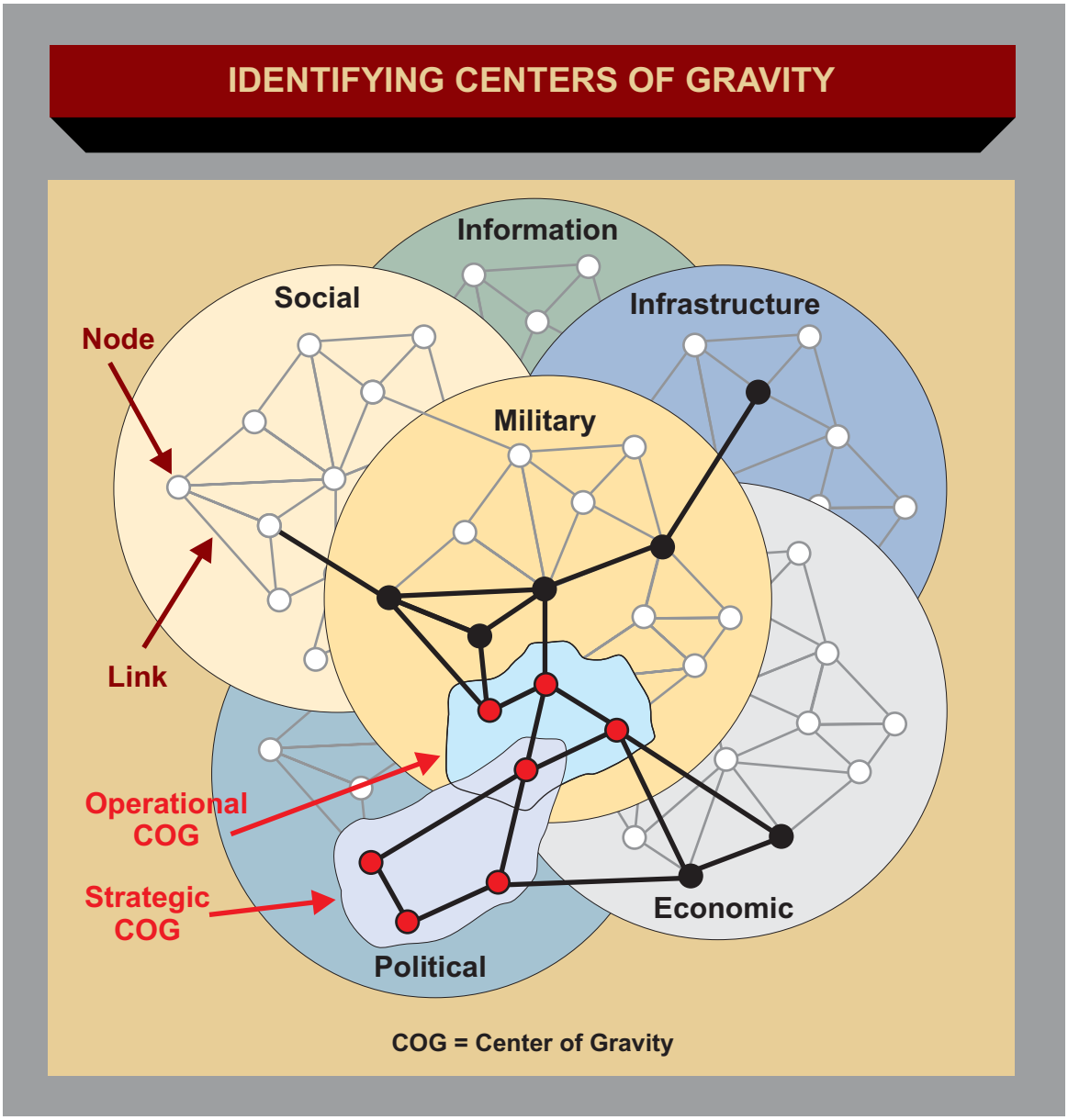


Figure IV-7. Identifying Centers of Gravity

and nodes associated with scientific research, commercial nuclear power generation, highly enriched uranium weapons development, and plutonium based weapons development. The situation templates may be combined, modeled, and compared to identify key nodes and primary and alternate links among nodes. The consolidated template (event template) provides the means for determining specific events in time and space that if detected would indicate changes in adversary behavior, systems, or the operational environment. These events, or indicators of change, may be assigned qualitative or quantitative thresholds and may be used as the basis for MOEs. Figure IV-8 is an example of a systems-oriented JIPOE event template demonstrating nodal and link analysis to identify potential indicators of change.

The JIPOE process and its relationship to assessment is described in greater detail in JP 2-01.3, Joint Intelligence Preparation of the Operational Environment.

17. Tactical-Level Assessment

Tactical-level assessment typically uses MOPs to evaluate task accomplishment. The results of tactical tasks are often physical in nature, but also can reflect the impact on specific functions and systems. Tactical-level assessment may include assessing progress by phase lines; neutralization of enemy forces; control of key terrain, people, or resources; and security or reconstruction tasks. Combat assessment is an example of a tactical-level assessment and is a term that can encompass many tactical-level assessment actions. Combat assessment typically focuses on determining the results of weapons engagement (with both lethal and nonlethal capabilities), and thus is an important component of joint fires and the joint targeting process. It helps the CCDR, the subordinate JFC, and component commanders understand how the joint operation is progressing and assists in shaping future operations. Combat assessments consist of a BDA, munitions effectiveness assessment (MEA), and reattack recommendation.

a. **Battle Damage Assessment.** BDA should be a timely and accurate estimate of damage or degradation resulting from the application of military force, lethal or nonlethal, against a target. **BDA is primarily an intelligence responsibility** with required inputs and coordination from operations and can be federated throughout the IC. It answers the question: "Were the strategic, operational, and tactical objectives met as a result of the forces employed against the selected targets?" **The most critical ingredient for effective BDA is a comprehensive understanding of the JFC's objectives and how they relate to a specific target.** For BDA to be meaningful, the JFC's objectives and the supporting MOEs must be observable, measurable, and obtainable. The JFC should provide a comprehensive plan, together with an intelligence architecture, to support BDA. This plan must synchronize ISR resources and reporting to effectively/efficiently support timely BDA. Preconflict planning requires collection managers with a thorough understanding of collection systems capabilities (both organic and national) as well as their availability. BDA consists of a physical damage assessment phase, functional damage assessment phase, and target system assessment phase.

(1) **Phase 1 — Physical Damage Assessment.** A physical damage assessment is an estimate of the quantitative extent of physical damage (through munitions blast, fragmentation and/or fire damage) to a target element based on observed or interpreted damage. This postattack target analysis should be a coordinated effort among combat units, component commands, the subordinate joint force,

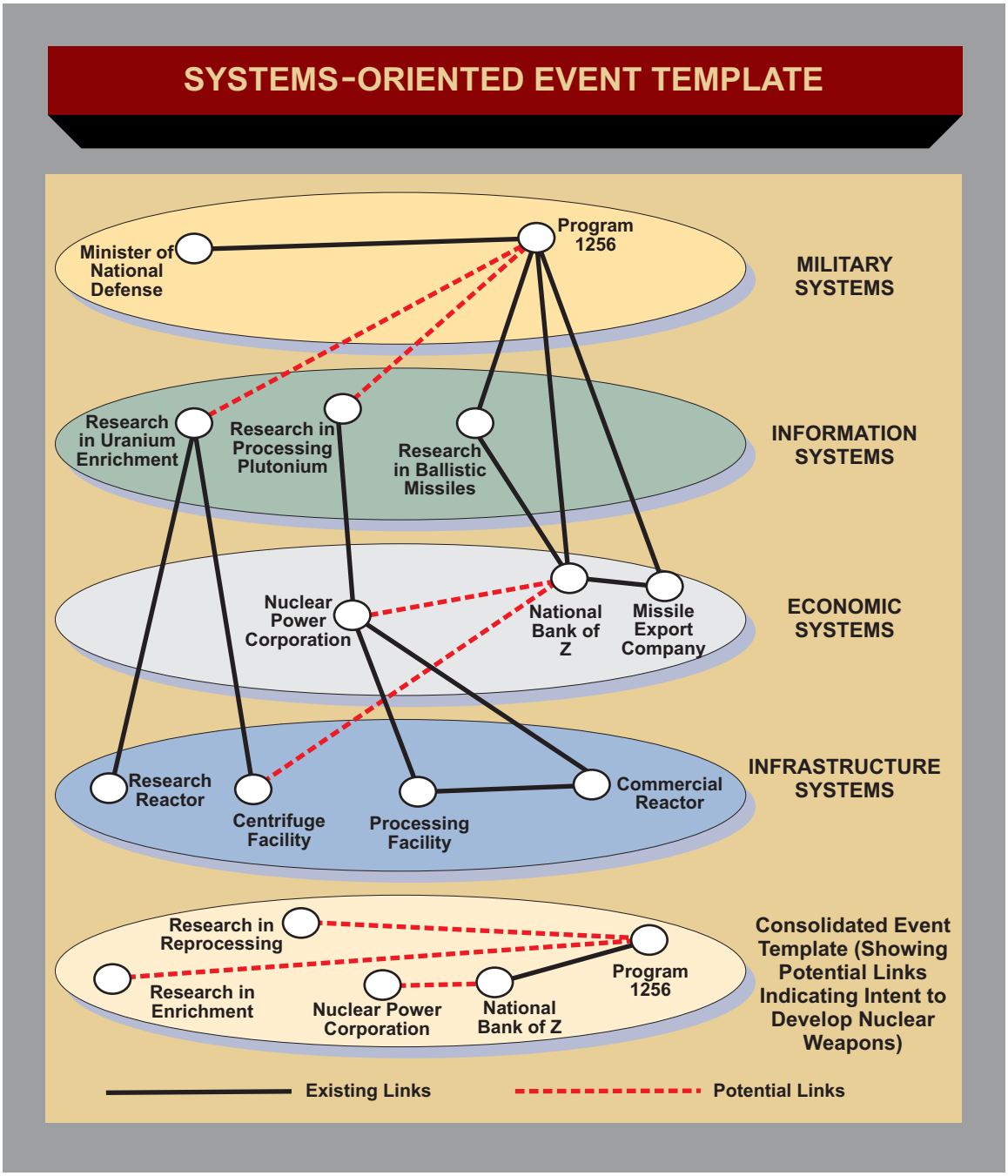


Figure IV-8. Systems-Oriented Event Template

the combatant command, national agencies, and other supporting organizations. The Joint Staff Targeting and BDA Cell, with J-2T as lead, serves as the national level BDA cell and coordinates combatant command BDA requirements with the IC. Some representative sources for data necessary to make a physical damage assessment include the air tasking order or master air attack plan, MISREPs, aircraft cockpit video, weapon system video, visual/verbal reports from ground spotters or combat troops, controllers and observers, artillery target surveillance reports, SIGINT, HUMINT, GEOINT, MASINT, and OSINT. Phase 1 BDA reporting contains an initial physical damage assessment of hit or miss based usually upon single source data.

(2) **Phase 2 — Functional Damage Assessment.** The functional damage assessment is an estimate of the effect of military force to degrade or destroy the functional/operational capability of a target to perform its intended mission. Functional assessments are inferred from the assessed physical damage and all-source intelligence information. This assessment must include an estimation of the time required for recuperation or replacement of the target's function. BDA analysts need to compare the original objective for the attack with the current status of the target to determine if the objective was met. Phase 2 BDA reporting builds upon the Phase 1 initial report and is a fused, all-source product addressing a more detailed description of physical damage, an assessment of the functional damage, inputs to target system assessment (Phase 3), and any applicable MEA comments. When appropriate, a reattack recommendation is also included.

(3) **Phase 3 — Target System Assessment.** Target system assessment is a broad assessment of the overall impact and effectiveness of military force applied against an adversary target system relative to the operational effects desired. These assessments may be conducted at the combatant command or national-level by fusing all Phase 1 and 2 BDA reporting on targets within a target system. Phase 3 BDA reporting contains an in-depth target system assessment. When appropriate, a reattack recommendation and/or targeting nomination is also included. This report combines the analyses from the Phase 1 and 2 reports, plus all-source information, and directly feeds back into the TSA.

b. **Munitions Effectiveness Assessment.** MEA is an assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and recommend any required changes to the methodology, tactics, weapon systems, munitions, fuzing, and/or delivery parameters to increase force effectiveness. MEA is conducted concurrently and interactively with BDA assessments. **MEA is primarily the responsibility of component operations, with inputs and coordination from the IC.** MEA targeting personnel seek to identify, through a systematic trend analysis, any deficiencies in weapon system and munitions performance or combat tactics by answering the question, "Did the systems (i.e., bomb or jamming) employed perform as expected?" Using a variety of intelligence and operations inputs, to include Phase 2 functional damage assessments, operators prepare a report assessing munitions performance and tactical applications. The report details weapon performance against specified target types. This information could have a crucial impact on future operations and the quality of future BDA. MEA can continue years after the conflict using archived data and information collected by on-site inspections of targets struck during the conflict.

c. **Reattack Recommendation (or Future Targeting Development).** BDA and MEA provide systematic advice on reattacking targets, culminates in a reattack recommendation and future targeting, and thus guide further target selection (or target development). Recommendations range from attacking different targets to changing munitions and/or delivery tactics. **The reattack recommendation and future targeting is a combined operations and intelligence function** and must be assessed against the relative importance of the target to the targeting effort/campaign being run.

For further information on combat assessment, see JP 3-60, Joint Targeting.

CHAPTER V
JOINT, INTERAGENCY, AND MULTINATIONAL INTELLIGENCE SHARING AND COOPERATION

"One of the most gratifying features of recent work in intelligence, and one that is quite unique in its long history, has been the growing cooperation established between the American intelligence services and their counterparts throughout the Free World which make common cause with us as we face a common peril."

Allen Dulles, *The Craft of Intelligence,* 1963

1. An Intelligence Sharing Environment

The success of joint and multinational operations and interagency coordination hinges upon timely and accurate information and intelligence sharing. A JFC must be capable of coordinating the actions of people, organizations, and resources at great distances among diverse participants, such as allies and coalition partners, OGAs, NGOs, and state and local authorities. To prevail, the JFC's decision-making and execution cycles must be consistently faster than the adversary's and be based on better information. Being faster and better requires having unfettered access to the collection, processing, and dissemination of information derived from **all** available sources. Information sharing, cooperation, collaboration, and coordination are enabled by an intelligence and information sharing environment that fully integrates joint, multinational, and interagency partners in a collaborative enterprise. This type of **collaborative intelligence sharing environment** must be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time. The architecture supporting this type of environment must be dynamic, flexible, and capable of providing multinational partners and interagency participants rapid access to appropriate data. It must facilitate the capability of the IC to focus on supporting the JFC and subordinate joint force components and to integrate support from non-DOD agencies and NGOs as needed. The intelligence sharing architecture is configured to provide the baseline data needed to support commanders at all levels. CCDRs are responsible for the intelligence sharing architecture for their commands. For contingency operations, subordinate JFCs, supported by their joint force J-2s, are responsible for establishing the joint force intelligence architecture required to accomplish the assigned mission.

a. **An intelligence sharing architecture is integral to all intelligence operations.** From planning and direction through dissemination and integration, the architecture supports intelligence functions over the Global Information Grid (GIG). The GIG employs a distributed global network involving various communications systems, computers, space-based intelligence support systems, and their associated resources and technologies.

b. **A collaborative intelligence sharing architecture must support the full range of military operations** and support the intelligence requirements of decision makers, from the President down through the joint force's tactical commanders. The architecture incorporates the policies, procedures, reporting structures, trained personnel, automated information processing systems, and connectivity to collect, process, and disseminate intelligence. It also provides support to natural or man-made disaster relief efforts that require military support.

2. Principles for Multinational Intelligence Sharing

"It's not a technical issue any more. It's really more about culture and the 'need to share' rather than the 'need to know."

General James Cartwright, USMC Commander, United States Strategic Command 6 April 2005

In most multinational operations, the JFC will be required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces. The JFC participating in the coalition or alliance must tailor the policy and procedures for that particular operation based on national and theater guidance. Intelligence efforts of the nations must be complementary and take into consideration the intelligence system strengths, limitations, and the unique and valuable capabilities each nation will have. In some multinational operations or campaigns, JFCs will be able to use existing international standardization agreements (e.g., North Atlantic Treaty Organization [NATO]) as a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation will be unique, such agreements may have to be modified or amended based on the situation. A JFC participating in a coalition or alliance must tailor the policy and procedures for that particular operation based on theater guidance and national policy as contained in National Disclosure Policy (NDP) 1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*. NDP 1 provides policy and procedures in the form of specific disclosure criteria and limitations, definition of terms, release arrangements, and other guidance. The following general principles (See Figure V-1) provide a starting point for creating the necessary policy and procedures:

a. **Maintain Unity of Effort.** Intelligence personnel of each nation need to view the threat from multinational as well as national perspectives. A threat to one element of an alliance or coalition by the common adversary must be considered a threat to all alliance or coalition elements. Success in intelligence

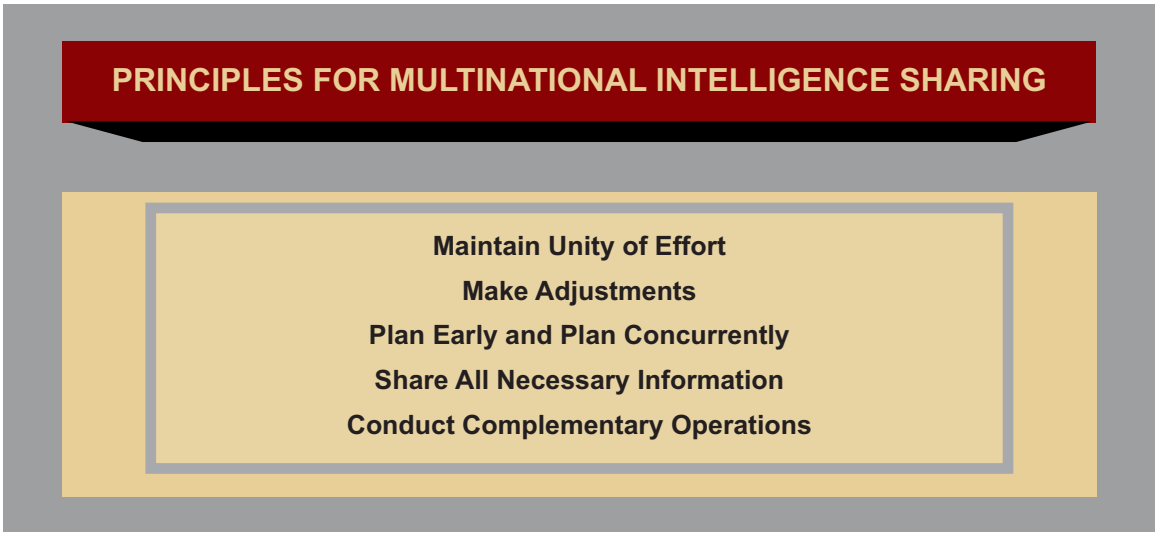


Figure V-1. Principles for Multinational Intelligence Sharing

sharing requires that we establish a trusted partnership with foreign counterparts to counter a common threat and maintain a unity of effort.

b. **Make Adjustments.** There will be differences in intelligence doctrine and procedures among the coalition partners. A key to effective multinational intelligence is readiness, beginning with the highest levels of command, to make the adjustments required to resolve significant differences. Major differences may include how intelligence is provided to the commander (jointly or individual Services or agencies), procedures for sharing information among intelligence agencies, and the degree of security afforded by different communications systems and procedures. Administrative differences that need to be addressed may include classification levels, personnel security clearance standards, requirements for access to sensitive intelligence, and translation requirements.

c. **Plan Early and Plan Concurrently.** JFCs need to determine what intelligence may be shared with the forces of other nations early in the planning process. NATO and the United States-Republic of Korea Combined Forces Command have developed and exercised intelligence policies and procedures that provide examples of how multinational planning can be done in advance.

d. **Share All Necessary Information.** Allies and coalition partners should share all relevant and pertinent intelligence about the situation and adversary consistent with NDP and theater guidance. However, information about intelligence sources and methods should not be shared with allies and coalition partners until approved by the appropriate national-level agency.

(1) In order to share critical intelligence information with allies and coalition partners efficiently, US intelligence information should be written for release at the lowest possible classification level and given the fewest possible dissemination restrictions within foreign disclosure guidelines. When information relating to a particular source cannot be shared, the intelligence derived from that source should still be provided to other coalition partners, so long as the information itself couldn't potentially compromise the source. The J-2 must establish procedures for separating intelligence from sources and methods. Intelligence production agencies often print highly classified reports in such a manner that compartmented information is separated from intelligence that can be widely disseminated by a "tear line" (the J-2 and component intelligence staff officers keep information above the tear line and disseminate the intelligence below). Having intelligence production agencies use such tear lines will greatly facilitate intelligence sharing.

(2) The joint force J-2 must obtain the necessary foreign disclosure authorization from DIA as soon as possible. J-2 personnel must be knowledgeable of the specific foreign disclosure policy, procedures, and regulations for the operation. The efficient flow of intelligence will be enhanced by the assignment of personnel knowledgeable of foreign disclosure.

(3) Force protection is a mission inherent to any commander, and intelligence support to that mission is critical. Every effort must be made to share any data that could impact the commander's force protection mission.

e. **Conduct Complementary Operations.** Intelligence efforts of each nation must be complementary. Each nation will have intelligence system strengths and limitations and unique and valuable capabilities. Host-nation security services' capabilities, for example, may contribute significantly to force protection. Furthermore, planning with friendly nations to fill shortfalls, especially linguist requirements, may help overcome such limitations. All intelligence resources and capabilities should be made available for application to the whole of the intelligence problem. Establishing a multinational collection management element is essential for planning and coordinating multinational collection operations.

Additional guidance on intelligence operations in multinational operations can be found in JP 2-01, Joint and National Intelligence Support to Military Operations. *Information on principles and constructs to support multinational operations can be found in JP 3-0,* Joint Operations*, and JP 3-16,* Multinational Operations.

3. Principles for Interagency Intelligence Collaboration

Interagency intelligence collaboration should be encouraged whenever possible consistent with applicable national, agency, or organizational procedures and classification guidelines. Successful interagency intelligence collaboration depends on many factors, to include: strong relationship networks, trust and respect among colleagues, sharing a common vision, minimizing territorial issues, continuous communication, and commitment from the leadership of collaborating organizations (See Figure V-2). Liaison personnel are instrumental in bridging gaps and working through barriers that may come up between organizations. An aggressive liaison effort is critical to developing and maintaining unity of effort from initial planning through the execution of operations. However, analysts must base their collaboration on classification, need-to-know, need-to-share, and applicable national, agency, or organizational guidelines.

a. **Establish Strong Relationship Networks.** Collaboration is built upon the relationships and networks of colleagues that analysts develop throughout their careers. Without knowledge of who one's counterparts are in other intelligence organizations, collaboration on intelligence problems is nearly impossible. Techniques for building relationship networks include attending or hosting conferences, visiting counterparts in other organizations, and exchanges of personnel through interorganizational rotational assignments.

b. **Build Mutual Trust and Respect for Colleagues.** As analysts work intelligence problems, they count on one another to share all relevant data from within their particular field of expertise. For example, imagery analysts should expect SIGINT analysts to provide all relevant information for a particular intelligence problem that they are working and vice versa. Trust and respect is facilitated by proactively communicating information to colleagues and counterparts and by ensuring they are recognized by their organizations for their expertise and contributions.

c. **Share a Common Vision.** A shared common vision should include the goal of providing the most comprehensive, accurate product possible to the customer. Individuals who develop or follow a personal agenda at the expense of other collaborators will, over time, be excluded from the collaborating

Figure V-2. Principles for Interagency Intelligence Collaboration

group. Sharing a common goal among collaborators is facilitated by taking the initiative to alert others when new information becomes available, working together instead of competing, and providing tip-offs of possible collection opportunities. By synchronizing efforts, the strengths of each organization can be maximized for the benefit of all collaborators.

d. **Minimize Territorial Issues.** Reducing the potential for interorganizational conflicts is vital to successful intelligence collaboration. It is important that analysts embarking on a collaborative effort recognize that turf issues are likely to occur and should not be ignored. These issues may be minimized by anticipating their occurrence, developing a plan for addressing them as they emerge, and stressing the mutually beneficial aspects of collaboration such as sharing organizational credit for the final product.

e. **Encourage Continuous Communication.** Continuous communication among intelligence colleagues and counterparts is critical to overcoming barriers to collaboration. Communication may be enhanced through frequent meetings, teleconferences, phone calls, mail, and e-mail, as well as less formal methods such as periodic working lunches.

f. **Eliminate Impediments.** The leadership of organizations involved in the collaborative enterprise should demonstrate their commitment by taking prompt and decisive action to eliminate any impediments to collaboration. Organizations should implement procedures to ensure incentives or consequences are instituted for cooperative or uncooperative behavior.

"Sometimes one agency simply does not recognize that a given piece of data would be of value to another. Too often, however, intelligence information is intentionally held so closely by the agency that collected and analyzed it that it is not shared with all of the parties who have a need to know…. Breaking down the bureaucratic barriers to effective intelligence sharing must be one of the highest priorities if we are to succeed in the campaign against terrorism."

Kurt M. Campbell and Michele A Flournoy,
To Prevail: An American Strategy for the Campaign
***Against Terrorism*, 2001**

4. Requirements and Standards for an Intelligence Sharing Architecture

a. **Requirements**. The intelligence sharing architecture must be capable of being tailored to support a specific JFC's information requirements. Intelligence must be provided in a form that is readily understood and directly usable by the recipient without providing the user irrelevant data.

(1) An effective intelligence sharing architecture requires a "reachback" capability — a means by which deployed military forces rapidly access information from, receive support from, and conduct collaboration and information sharing with other units (deployed in theater and from outside the theater). **Dissemination of intelligence consists of both "push" and "pull" control principles.** The **"push"** construct allows the higher echelons to push intelligence down to satisfy existing lower echelon requirements or to relay other relevant information to the lower level. The **"pull"** construct involves direct electronic access to databases, intelligence files, or other repositories by intelligence organizations at all levels. "Push" updates must be based on the JFC's PIRs and other intelligence requirements to ensure that the JFC receives critical information and intelligence. Higher echelons should be aware of PIRs at lower echelons and push PIR related intelligence rather than requiring lower echelons to pull the intelligence. Other information must be available on an as-needed "pull" basis so that the joint force J-2 avoids information overload. From the Secretary of Defense through the tactical commanders, the architecture must provide complete, tailored, all-source intelligence to the decision maker.

"Push" and "pull" control principles are discussed in detail in JP 2-01, Joint and National Intelligence Support to Military Operations.

(2) The intelligence sharing architecture should be **constructed so there is no single point of failure.** At the same time, the architecture must identify and eliminate any unnecessary duplication of intelligence capabilities so that scarce resources can be focused to meet prioritized requirements.

(3) The intelligence sharing architecture **must accommodate the widest possible range of missions and operational scenarios.** It must respond to the JFC's requirements for information at any time and any place and support multinational operations with no loss in timeliness. The intelligence operational architecture must incorporate the capabilities of the national and Service intelligence organizations, and provide to the JTF and its components the capability to access national and Service capabilities when necessary.

(4) The intelligence sharing architecture must **achieve a seamless integration of the JFC's decision-making and execution cycles with the intelligence process.** In developing the operational architecture, the IC must streamline the intelligence process to ensure responsiveness to the JFC's requirements.

(5) The intelligence sharing architecture must be **developed so that users can train and exercise with intelligence capabilities in peacetime.** Intelligence systems, policies, procedures, connectivity, security, and fusion requirements must be part of joint training exercises and are incorporated into simulations. During exercises, capabilities must function exactly as in a real operation, so that the users train in a realistic, seamless environment. The architecture must be configured so that real world databases are preserved and cannot be accidentally or maliciously altered during an exercise.

(6) The intelligence architecture must **provide for integration with existing and projected secure teleconferencing and other collaborative communication capabilities.** Secure teleconferencing will permit groups of dispersed users to collaborate during the planning and execution of intelligence operations and to coordinate with operational users. Dispersed users include, but are not limited to, JFCs and their subordinate commanders, the DJIOC and theater JIOCs, JTF JISE, the multinational intelligence center and/or appropriate multinational partners, the Joint Staff, Services, the combat support agencies, OGAs, and national decision makers.

> *"When time-sensitive intelligence cannot be relayed quickly and reliably to those who need it most, it is of negligible value in the fast-paced environment of the modern battlefield. Success in solving this problem, which is as technical as it is organizational, requires meticulous planning and thorough testing."*
>
> **Michael I. Handel**
> **Professor of National Security and Strategy, Army War College**
> **Intelligence and Military Operations, 1990**

b. **Standards**. The intelligence sharing architecture must meet established standards for survivability, interoperability, security, and compatibility.

(1) **Survivability.** The system design specified in the technical architecture must be as survivable as the command structure it supports. Assets that are vulnerable to damage or destruction must have alternative means of providing required data with minimal risk.

(2) **Interoperability.** It is imperative that intelligence and operations systems architectures be fully interoperable in order to facilitate a COP. The systems architecture should comply with DOD joint net-centric standards. The technical architecture must be designed to accommodate interoperability and integration with existing and projected intelligence information systems and with those joint systems that must exchange information with the intelligence technical architecture.

(3) **Security.** Information must be protected in accordance with mandatory security polices. The architecture must be designed so that the widest possible access is permitted without compromising security.

(4) **Compatibility.** The architecture must use common data formats when reengineering existing systems or applications and developing new systems. As a mid-term objective, all components' intelligence systems must be capable of exchanging data, information and intelligence products to allow all-source analysis and fusion. This capability to share data and information must extend to applications, databases, and communications protocols to ensure that intelligence information is compatible with work stations, file servers, and communications links. Both anticipated and unanticipated authorized users must have access to the discoverable, understandable information required to adapt to situations more quickly than the enemy.

c. **Responsibilities.** In coordination with the Joint Staff, national intelligence agencies, OSD, Defense Information Systems Agency, and Military Service intelligence organizations, DIA is responsible for implementing, managing, and ensuring compliance with the configuration of information, data, and communications standards for DOD intelligence systems. DIA establishes defense-wide intelligence priorities for attaining interoperability between the tactical, theater, and national intelligence systems and the respective communications systems at each level.

5. Components of an Intelligence Sharing Architecture

a. Organizational Structures

(1) **In multinational operations**, the multinational force commander exercises command authority over a military force composed of elements from two or more nations. The President retains command authority over US forces, but may place appropriate forces under the operational control of a foreign commander to achieve specific military objectives. However, any large-scale participation of US forces in a major operation will likely be conducted under US command and operational control or through accepted and stable regional security organizations such as NATO. Therefore, in most multinational operations, the JFC will be required to share intelligence with foreign military forces and to coordinate receiving intelligence from those forces. In some circumstances, the JFC will need to seek authority to go outside the usual political-military channels to provide information to NGOs. Unique intelligence policy and dissemination criteria will have to be tailored to each multinational operation.

(a) A multinational intelligence center is necessary for merging and prioritizing the intelligence requirements from each participating nation and for acquiring and fusing all the nations' intelligence contributions. Likewise, the center should coordinate the intelligence collection planning and ISR operations of each nation. The multinational intelligence center should include representatives from all nations participating in the multinational operation. Designating a single director of intelligence for the multinational command will greatly assist in resolving potential disagreements among the multinational members. Figure V-3 depicts a notional multinational intelligence architecture.

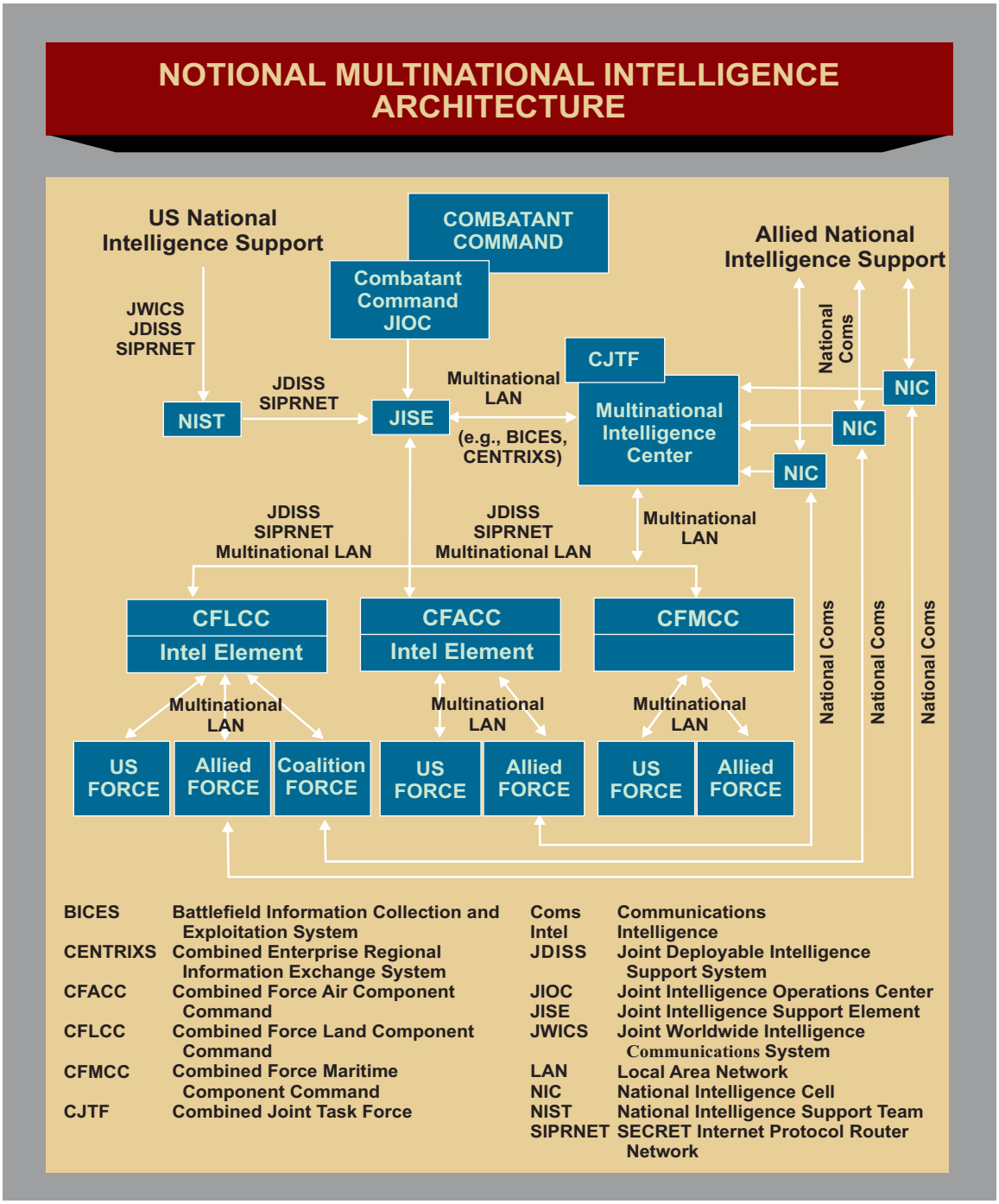


Figure V-3. Notional Multinational Intelligence Architecture

(b) Intelligence liaison is critical between commands and among supporting and supported organizations. Liaison personnel are instrumental in resolving problems resulting from language barriers and cultural and operational differences that normally occur in multinational operations. Because of the inherent complexities associated with multinational operations, an aggressive liaison effort is critical to developing and maintaining unity of effort. A robust liaison effort with sufficient communications is particularly critical in the initial stages of planning and forming a coalition, particularly when the US

Multinational personnel are briefed during Combined Endeavor – a 35 nation exercise to test communication interoperability.

intelligence network is not yet established. US SOF may be assigned down to coalition brigade level to act as coalition liaison elements or support teams. These teams have the ability to receive and disseminate intelligence directly to and from their counterparts. The team members are selected based upon their language and cultural knowledge of the area and are in direct communication with either their combined joint special operations task force, or the next higher special operations command and control element.

(2) **During interagency coordination,** information and intelligence sharing are facilitated by each combatant command's JIOC, DNI representative, DFE, and joint interagency coordination group (JIACG).

(a) The combatant command JIOC is the theater focal point for planning, synchronizing, coordinating, and integrating the full range of intelligence operations in the command's AOR. The JIOC works with the DNI representative to the combatant command and liaison personnel from DOD and non-DOD national intelligence organizations to ensure all relevant intelligence and information is fully shared in the most timely manner possible.

(b) The JIACG facilitates the application of the instruments of national power in a coherent manner and provides a means to integrate interagency perspective into military planning and execution. The JIACG, consisting of representatives from OGAs, serves as a multifunctional advisory element that can facilitate information sharing, operational-level planning and coordination, and political-military synthesis across the interagency community for the CCDR and staff. A typical JIACG may connect to the various US embassies and their country teams as well as to national-level planners. Its primary role is to bridge the gap between civilian agency and military

campaign planning efforts for regional engagement and potential regional crises. Specific objectives of the JIACG are to:

1. Improve operational interagency planning and execution.

2. Exercise secure collaboration processes and procedures with participating agencies.

3. Promote continuous relationships among interagency planners.

Further information on the JIACG is contained in JP 3-08, Interagency Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations.

b. **Systems Network**. **A network of integrated work stations, file servers, and communications links** comprises the second component of an integrated intelligence architecture. The components of the systems network must work together and comply with the evolving defense information infrastructure, COP, net centric data strategies, and DOD Information Technology Standards Registry, to create the interoperable collaborative information environment required to support joint and multinational operations and interagency coordination. The network includes direct connectivity by appropriate communications or communications relay link (landline, radio, satellite, and others as appropriate) and broadcast capability to support time-sensitive needs.

(1) The GIG allows data collected by any means to be communicated directly to a user or to a processing site or platform by the most efficient path, then passed on or through to the user as appropriate. A critical aspect of the information grid is its ability to make all intelligence accessible by way of standardized file servers to standards-compliant workstations.

(2) The DOD Intelligence Information System Enterprise is the global set of resources (people, facilities, hardware, software, and processes) that provide information technology and information management services to the DOD military intelligence community through a tightly-integrated, interconnected and geographically distributed regional service center architecture. The enterprise capabilities are centrally managed and de-centrally executed under the authority and direction of the DIA Chief Information Officer.

(3) To maximize the utility of the systems architecture, systems must be interoperable. Standard communications protocols and standard encryption devices must be available at all echelons. The systems architecture should have the flexibility to accommodate, not replace, existing I&W and direct support systems. The systems architecture is intended to be sufficiently agile to allow updating with innovative technology or to overlay additional capabilities using existing communications carriers. Until an effective multilevel security system is in place with joint forces, the intelligence architecture must support three possible levels of information: SCI, non-SCI (TOP SECRET and below), and intelligence releasable to allies and coalition partners.

Joint Worldwide Intelligence Communications System

Joint Worldwide Intelligence Communications System (JWICS) is a sensitive compartmented information element of the Defense Information System Network. JWICS incorporates advanced networking technologies that permit point-to-point or multi-point information exchange involving voice, text, graphics, data, and video teleconferencing.

(a) **SCI Support.** JWICS and JDISS currently form the common baseline for all SCI support systems in the intelligence architecture.

1. **JWICS** satisfies the requirement for secure, high-speed, multimedia transmission services for SCI. JWICS incorporates advanced networking technologies that permit greater throughput and capacity, making possible the use of applications that take advantage of multimedia technologies including video teleconferencing. Video-capable JWICS nodes can create, receive, transmit, and store video images as well as voice, text, graphics, and data. Information can be either broadcast or shared interactively among JWICS subscribers on a point-to-point or multi-point basis. The JWICS circuit can be managed by way of allocation of bandwidth, allowing simultaneous use of the link for multiple applications.

2. **JDISS** provides the standard workstation server software configuration. The basic backbone for the dissemination of intelligence to and from deployed JDISS nodes is the JWICS network. Where JWICS is not required or not available, JDISS has a versatile communications capability that can interface with existing communications systems, such as tri-Service tactical communications systems. The system architecture optimizes flexibility to focus intelligence efforts efficiently and ensures that support is maximized for a joint force engaged in military operations.

Combined Enterprise Regional Information Exchange System (CENTRIXS)

"US Central Command (USCENTCOM) established a Coalition Intelligence Center (CIC)... to leverage the access, intelligence expertise and perspectives of our 68 Operation ENDURING FREEDOM Coalition partners. Intelligence representatives from traditional Commonwealth and North Atlantic Treaty Organization partners (United Kingdom, Canada, Australia, New Zealand, Germany, Denmark, France) were integrated into daily operations on a more comprehensive basis; useful terrorism exchange relationships were established with several nontraditional partners resident at USCENTCOM Headquarters, to include Russia, Uzbekistan and Ethiopia. The Combined Enterprise Regional Information Exchange System (CENTRIXS) [was] designed for exactly this type of scenario.... CENTRIXS links into Global Command & Control System Common Operation Picture servers and facilitates operations/intelligence sharing at releasable levels through use of multilevel database replication guards, facilitating rapid Coalition access to US databases without human intervention. Coalition

partners have given the system high marks and access daily products for local and national decision maker situational awareness…. This is a 'big deal' in terms of information superiority – we simply cannot move very far ahead without enforced standards, discipline and sustained funding emphasis in this regard."

Brigadier General John F. Kimmons, USA
Director of Intelligence, USCENTCOM
Testimony to the US House of Representatives
Permanent Select Committee on Intelligence
23 May 2002

(b) **Non-SCI Support.** The SECRET Internet Protocol Router Network, Non-Secure Internet Protocol Router Network, and Global Command and Control System provide common non-SCI support systems for joint forces and interagency partners.

(c) **Multinational Support.** Multinational intelligence sharing should be facilitated by establishing a shared local area network using systems such as the Battlefield Information Collection and Exploitation System or the Combined Enterprise Regional Information Exchange System (CENTRIXS). As the current DOD multinational information-sharing portion of the GIG, CENTRIXS defines the standards for establishing and maintaining multinational connectivity at the tactical and operational level, with reachback capability to the strategic level.

c. **Standardized procedures** for disseminating and exchanging intelligence constitute the third component of an intelligence sharing architecture. These procedures are critical to joint and multinational operations and interagency coordination.

(1) The procedures and methodology for intelligence and information sharing should be conceived and exercised as part of multinational and interagency planning before operations begin. Special attention should be paid to intelligence classification and levels of access of multinational personnel. To this end, the J-2 should consider adding extra foreign disclosure officer billets to facilitate information sharing. The effectiveness of the procedures and methodology should be monitored and, when necessary, adapted during operations to meet changing circumstances.

EXAMPLES OF MULTINATIONAL INTELLIGENCE SHARING LEVELS

Procedures established to support US and United Nations (UN) forces in Somalia as members of the UN Operations in Somalia (UNOSOM II) effort used two levels of intelligence: Level 1 data could be shown to but not retained by coalition forces or the UN, while Level 2 data was cleared for release to the coalition and the UN. Level 1 intelligence remained within US-only channels, while Level 2 data flowed to the UNOSOM II information center in Mogadishu either from the UN Headquarters or via the US joint intelligence support element.

In some situations there may be more than two levels of intelligence required. For example, an operation involving a mixture of North Atlantic Treaty Organization (NATO) and non-NATO forces could have "US Only," "Releasable to NATO," and "Releasable to Non-NATO" levels. The multinational force commander (MNFC) will play a major role in advising the national intelligence community on the intelligence requirements for each of the allies and coalition partners. The MNFC will need to recommend what intelligence should be provided to each member.

(2) Following established guidelines, data should be passed to standardized data stores as soon as possible. In some situations the data will require processing and exploitation to convert it into a format compatible with certain storage means. However, whenever possible, data not requiring prior conversion should be automatically passed to the standardized data stores without processing. Automated posting of data combined with flexible connectivity to computer systems at all echelons of the command structure and within the Services allow intelligence analysts access to imagery and multiple databases while concurrently producing intelligence products in response to specific mission requirements. For example, high-resolution video collected by an unmanned aerial system can be viewed in near real time at a downlink processing site, but disseminating this video requires high bandwidth. The unprocessed video can be relayed directly by fiber optic line or satellite to a headquarters' element or JTF JISE. At the same time, targeting information can be reported to tactical elements by voice communications or message. Selected video frames can be captured by JDISS and made available to all users over the intelligence architecture. Information processed by a headquarters element or JTF JISE could, in turn, be transmitted or made available by JWICS and/or JDISS. In this example, all the capabilities linked to and by the intelligence sharing architecture are exercised including both "pull" and "push" dissemination. The information is made available for a variety of users' needs and is included in products and reports that serve multiple purposes for the tactical users.

APPENDIX A
INTELLIGENCE CONFIDENCE LEVELS

1. The J-2 should distinguish between what is known with confidence based on the facts of the situation and the adversary and what are untested assumptions. Intelligence can be facts that have been observed, or it can be a conclusion based on facts of such certainty that it is considered to be knowledge. Intelligence can also be conclusions and estimates deduced from incomplete sets of facts or induced from potentially related facts. The commander's determination of appropriate objectives and operations may rest on knowing whether intelligence is "fact" or "assumption," and knowing the particular logic used to develop an intelligence estimate, as well as knowing the confidence level the J-2 places on the provided intelligence and related analytic conclusions.

2. The following chart (Figure A-1) is intended to illustrate confidence levels intelligence personnel may use to indicate a subjective judgment regarding the degree of confidence they place on the analytic conclusions contained in intelligence products. Confidence levels may be used by intelligence producers to present analysis and conclusions to decision makers in a uniform, consistent manner. Because analytic conclusions are the products of source reliability and the analyst's experience, judgment and intuition, the confidence-level scale gives both a verbal and numerical value to be used as a shorthand assessment for the JFC. When using the verbal descriptors, analysts should ensure that commanders and other intelligence users are explicitly aware of the corresponding numerical value. The numerical side of the scale should prove more useful in a multinational operations situation. The "highly unlikely" confidence level permits the reporting of all information gathered, even if the reporter has a low opinion of its accuracy.

INTELLIGENCE CONFIDENCE LEVELS

Description of Probability or Confidence	Synonyms	Percent
HIGHLY LIKELY	◆ Highly Probable ◆ We Are Convinced ◆ Virtually Certain ◆ Almost Certain ◆ High Confidence ◆ High Likelihood	>90%
LIKELY	◆ Probable ◆ We Estimate ◆ Chances Are Good ◆ High-Moderate Confidence ◆ Greater Than 60% Likelihood	60-90%
EVEN CHANCE	◆ Chances Are Slightly Greater (or Less) Than Even ◆ Chances Are About Even ◆ Moderate Confidence ◆ Possible	40-60%
UNLIKELY	◆ Probably Not ◆ Not Likely ◆ Improbable ◆ We Believe ...Not ◆ Low Confidence ◆ Possible but Not Likely	10-40%
HIGHLY UNLIKELY	◆ Highly Improbable ◆ Nearly Impossible ◆ Only a Slight Chance ◆ Highly Doubtful	<10%

Figure A-1. Intelligence Confidence Levels

APPENDIX B
INTELLIGENCE DISCIPLINES

1. Geospatial Intelligence

GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, IMINT, and geospatial information. GEOINT encompasses a range of products from simple IMINT reports to complex sets of layered foundation and intelligence/mission-specific data. GEOINT products are often developed through a "value added" process, in which both the producer and the user of GEOINT update a database or product with current information. Advanced geospatial intelligence (AGI), formerly known as imagery-derived MASINT, includes all types of information technically derived from the processing, exploitation, and non-literal analysis. AGI does not include the MASINT subelements of radio-frequency, materials, nuclear radiation, geophysical, or radar not related to synthetic aperture radar. The three components of GEOINT (imagery, IMINT and geospatial information) are discussed below.

a. **Imagery** is a likeness or presentation of any natural or man-made feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likenesses or presentations produced by satellites, airborne platforms, unmanned aerial vehicles, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of HUMINT collection organizations). It is used extensively to update GEOINT foundation data and serves as GEOINT's primary source of information when exploited through IMINT. Imagery comes in two formats: conventional (film-based, hardcopy, sometimes transferred to electronic format) or electronic (digital, softcopy) as either still or motion. Electronic offers many advantages over conventional including improved timeliness, greater dissemination options, and additional imagery enhancement and exploitation capabilities.

b. **IMINT** is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. It includes exploitation of imagery data derived from electro-optical (EO), radar, infrared (IR), multi-spectral, and laser sensors. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media. The joint force is able to draw support from a number of platforms and sensors with differing capabilities.

(1) **EO sensors** provide digital imagery data in the IR, visible, and/or ultraviolet regions of the electromagnetic spectrum. EO sensors operating in the visible spectrum can provide a high level of detail or resolution but cannot successfully image a target in darkness or, as with EO sensors in general, bad weather. EO offers many advantages over non-digital (i.e., film-based) systems including improved timeliness, greater dissemination options, imagery enhancement, and additional exploitation methods.

(2) **Radar imaging sensors** provide all weather imaging capabilities and the primary night capability. Radar imagery is formed from reflected energy in the radio frequency portion of the electromagnetic spectrum. Some radar sensors provide moving target indicator capability to detect and locate moving targets such as armor and other vehicles.

(3) **IR imaging sensors** provide a pictorial representation of the contrasts in thermal IR emissions between objects and their surroundings, and are effective during periods of limited visibility such as at night or in inclement weather. A unique capability available with IR sensing is the ability to capture residual thermal effects.

(4) **Spectral imagery sensors** operate in discrete spectral bands, typically in the IR and visible regions of the electromagnetic spectrum. Spectral imagery is useful for characterizing the environment or detecting and locating objects with known material signatures. Some **multispectral imagery (MSI)** sensors provide low resolution, large area coverage that may reveal details not apparent in higher resolution EO imagery. Map-like products can be created from MSI data for improved area familiarization and orientation. **Hyperspectral imagery (HSI)** is derived from subdividing the electromagnetic spectrum into very narrow bandwidths which may be combined with, or subtracted from each other in various ways to form images useful in precise terrain or target analysis. For example, HSI can analyze electromagnetic propagation characteristics, detect industrial chemical emissions, identify atmospheric properties, improve detection of blowing sand and dust, and evaluate snow depths.

(5) **Light detection and ranging (LIDAR) sensors** are similar to radar, transmitting laser pulses to a target and recording the time required for the pulses to return to the sensor receiver. LIDAR can be used to measure shoreline and beach volume changes, conduct flood risk analysis, identify waterflow issues and augment transportation mapping applications. LIDAR supports large scale production of high-resolution digital elevation products displaying accurate, highly detailed three-dimensional models of structures and terrain invaluable for operational planning and mission rehearsal.

c. **Geospatial information** identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data; information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data, and related products. This information is used for military planning, training, and operations including navigation, mission planning and rehearsal, modeling and simulation, and targeting.

GEOINT is addressed in detail in JP 2-03, Geospatial Intelligence Support to Joint Operations.

2. Human Intelligence

HUMINT is a category of intelligence derived from information collected and provided by human sources. This includes all forms of information gathered by humans, from direct reconnaissance and observation to the use of recruited sources and other indirect means. This

discipline also makes extensive use of biometric data (e.g., fingerprints, iris scans, voice prints, facial/physical features) collected on persons of interest.

a. **Interrogation.** Interrogation is the systematic effort to procure information to answer specific collection requirements by direct and indirect questioning techniques of a person who is in the custody of the forces conducting the questioning. Proper questioning of enemy combatants, enemy prisoners of war, or other detainees by trained and certified DOD interrogators may result in information provided either willingly or unwittingly.

There are important legal restrictions on interrogation and source operations. Federal law and Department of Defense policy require that these operations be carried out only by specifically trained and certified personnel. Violators may be punished under the Uniform Code of Military Justice.

b. **Source Operations.** Designated and fully trained military HUMINT collection personnel may develop information through the elicitation of sources, to include:

(1) **"Walk-in" sources**, who without solicitation make the first contact with HUMINT personnel.

(2) **Developed sources** that are met over a period of time and provide information based on operational requirements.

(3) **Unwitting persons**, with access to sensitive information.

c. **Debriefing.** Debriefing is the process of questioning cooperating human sources to satisfy intelligence requirements, consistent with applicable law. The source usually is not in custody and usually is willing to cooperate. Debriefing may be conducted at all echelons and in all operational environments. Through debriefing, face-to-face meetings, conversations, and elicitation, information may be obtained from a variety of human sources, such as:

(1) **Friendly forces personnel**, who typically include high-risk mission personnel such as combat patrols, aircraft pilots and crew, long range surveillance teams, and SOF, but can include any personnel with information that can be used for intelligence analysis concerning the adversary or other relevant aspects of the operational environment. Combat intelligence, if reported immediately during an operational mission, can be used to redirect tactical assets to attack enemy forces on a time sensitive basis.

(2) **Refugees/displaced persons**, particularly if they are from enemy controlled areas of operational interest, or if their former placement or employment gave them access to information of intelligence value.

(3) **Returnees**, including (returned prisoners of war and defectors, freed hostages, and personnel reported as missing in action).

(4) **Volunteers**, who freely offer information of value to US forces on their own initiative.

d. **Document and Media Exploitation.** Captured documents and media, when properly processed and exploited, may provide valuable information such as adversary plans and intentions, force locations, equipment capabilities, and logistical status. The category of "captured documents and media" includes all media capable of storing fixed information to include computer storage material. This operation is not a primary HUMINT function, but may be conducted by any intelligence personnel with appropriate language support.

HUMINT is addressed in detail in JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations.

3. Signals Intelligence

SIGINT is intelligence produced by exploiting foreign communications systems and noncommunications emitters. SIGINT provides unique intelligence information, complements intelligence derived from other sources and is often used for cueing other sensors to potential targets of interest. For example, SIGINT which identifies activity of interest may be used to cue GEOINT to confirm that activity. Conversely, changes detected by GEOINT can cue SIGINT collection against new targets. The discipline is subdivided into three subcategories: **communications intelligence (COMINT), ELINT, and foreign instrumentation signals intelligence (FISINT).**

a. **COMINT** is intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means. COMINT includes computer network exploitation, which is gathering data from target or adversary automated information systems or networks. COMINT also may include imagery, when pictures or diagrams are encoded by a computer network/radio frequency method for storage and/or transmission. The imagery can be static or streaming.

b. **ELINT** is intelligence derived from the interception and analysis of noncommunications emitters (e.g., radar). ELINT consists of two subcategories; operational ELINT (OPELINT) and technical ELINT (TECHELINT). **OPELINT** is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems. **TECHELINT** is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.

c. **FISINT** involves the technical analysis of data intercepted from foreign equipment and control systems such as telemetry, electronic interrogators, tracking/fusing/arming/firing command systems, and video data links.

4. Measurement and Signature Intelligence

MASINT is scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydro-magnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target, source, emitter, or sender. The measurement aspect of MASINT refers to actual measurements of parameters of an event or object such as the demonstrated flight profile and range of a cruise missile. Signatures are typically the products of multiple measurements collected over time and under varying circumstances. These signatures are used to develop target classification profiles and discrimination and reporting algorithms for operational surveillance and weapon systems. The technical data sources related to MASINT include:

a. **EO data -** emitted or reflected energy across the visible/IR portion of the electromagnetic spectrum (ultraviolet, visible, near IR, and IR).

b. **Radar data -** radar energy reflected (reradiated) from a target or objective.

c. **Radio frequency data -** radio frequency/electromagnetic pulse emissions associated with nuclear testing, or other high energy events for the purpose of determining power levels, operating characteristics, and signatures of advanced technology weapons, power, and propulsion systems.

d. **Geophysical data -** phenomena transmitted through the Earth (ground, water, atmosphere) and man-made structures including emitted or reflected sounds, pressure waves, vibrations, and magnetic field or ionosphere disturbances. Subcategories include seismic intelligence, acoustic intelligence, and magnetic intelligence.

e. **Materials data -** gas, liquid, or solid samples, collected both by automatic equipment, such as air samplers, and directly by humans.

f. **Nuclear radiation data -** nuclear radiation and physical phenomena associated with nuclear weapons, processes, materials, devices, or facilities.

5. Open-Source Intelligence

OSINT is based on publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access. Examples of OSINT include on-line official and draft documents, published and unpublished reference materiel, academic research, databases, commercial and noncommercial websites, "chat rooms," and web logs ("blogs"). OSINT complements the other intelligence disciplines and can be used to fill gaps and provide accuracy and fidelity in classified information databases. However, caution should be exercised when using OSINT in that open sources may be susceptible to adversary use as a mode of deception (e.g., incorrect information may be planted in

public information). All-source intelligence should combine, compare, and analyze classified and open source materiel to provide the full context and scope of the information needed to support US forces.

a. Routine needs for OSINT may be satisfied by querying organization and intelligence community resources to retrieve available information. These resources include commercial on-line information databases and products such as Jane's Yearbooks, Library of Congress country studies, and the NSA telecommunication database, libraries, organization databases containing unclassified information, Internet searches, and the DNI Open Source Center (including the former Foreign Broadcast Information System) products and services.

b. OSINT is very useful **during interagency collaboration and in multinational operations where intelligence information based on OSINT sources can be easily shared**. However, caution must be exercised to ensure that intelligence sharing arrangements, to include the sharing of OSINT source products, have been approved through the JFC's foreign disclosure office. OSINT can be particularly important during peace operations that place a premium on human factors analysis and data derived from sociological, demographic, cultural, and ethnological studies. By using OSINT to supply basic information, controlled assets and/or resources and technical systems are freed to be directed against priority intelligence gaps. Open source material is useful in support of all kinds of military operations, and **is particularly useful where the US Government has minimal or no official presence**. For example, DOD intelligence production analysts use open source information on bridge loads, railroad schedules, electric power sources, and other logistics related topics to support US troop transport operations and noncombatant evacuation operations. Understanding the use of deception or misinformation in certain open source media are also key to productive employment of OSINT information.

6. Technical Intelligence

TECHINT is derived from the exploitation of foreign materiel and scientific information. TECHINT begins with the acquisition of a foreign piece of equipment or foreign scientific/technological information. The item or information is then exploited by specialized, multi-Service collection and analysis teams. These TECHINT teams assess the capabilities and vulnerabilities of captured military materiel and provide detailed assessments of foreign technological threat capabilities, limitations, and vulnerabilities.

a. TECHINT products are used by US weapons developers, countermeasure designers, tacticians, and operational forces to prevent technological surprise, neutralize an adversary's technological advantages, enhance force protection, and support the development and employment of effective countermeasures to newly identified adversary equipment. At the strategic level, the exploitation and interpretation of foreign weapon systems, materiel, and technologies is referred to as scientific and technical intelligence (S&TI).

b. The DIA provides enhanced S&TI to CCDRs and their subordinates through the Technical Operational Intelligence (TOPINT) program. TOPINT uses a closed loop system that integrates all Service and DIA S&T centers in a common effort. The TOPINT program provides timely

collection, analysis, and dissemination of theater specific S&TI to CCDRs and their subordinates for planning, training, and executing joint operations.

7. Counterintelligence

CI is similar to, and often confused with, HUMINT, as CI uses many of the same techniques for the information collection. CI obtains information by or through the functions of CI operations, investigations, collection and reporting, analysis, production, dissemination, and functional services. CI is not solely a collection discipline, however, and also acts upon information for both offensive and defensive purposes, in coordination with other intelligence disciplines, law enforcement and/or security elements.

a. The function of CI is to provide direct support to operational commanders, program managers, and decision makers. This support includes: CI support to force protection during all types and phases of military operations; detection identification and neutralization of espionage; antiterrorism; threat assessments; counterproliferation actions associated with CBRNE; countering illegal technology transfer; acquisitions systems protection; support to other intelligence activities; information systems protection; and treaty support.

b. Although CI is an activity separate and distinct from foreign intelligence, it supports the foreign intelligence disciplines through its contribution to the I&W function, by its collection, analysis, and production capabilities, and by maintenance of CI databases.

CI is addressed in detail in JP 2-01.2, Counterintelligence and Human Intelligence Support to Joint Operations.

Intentionally Blank

APPENDIX C
REFERENCES

The development of JP 2-0 is based upon the following primary references.

1. General

a. Title 10, US Code, *Armed Forces*.

b. Title 50, US Code, *War and National Defense*.

c. The National Security Act of 1947.

d. The Goldwater-Nichols Department of Defense Reorganization Act of 1986.

e. The United Nations Participation Act.

f. NDP 1, *National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations*.

g. EO 12333, *United States Intelligence Activities*.

h. Director Central Intelligence Directive 7/3, *Information Operations and Intelligence Community Related Activities*.

2. Department of Defense

a. Secretary of Defense Memorandum, "Strengthening Defense Intelligence."

b. DOD Directive 3600.1, *Information Operations (IO)*.

c. DOD Directive 5100.1, *Functions of the* Department of Defense and its Major Components.

d. DOD Directive 5240.1, *DOD Intelligence Activities*.

e. DOD 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons.*

3. Chairman of the Joint Chiefs of Staff

a. CJCSI 5120.02, *Joint Doctrine Development System*.

b. JP 1, *Doctrine for the Armed Forces of the United States*.

c. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*.

d. JP 2-01, *Joint and National Intelligence Support to Military Operations*.

e. JP 2-01.2, *Counterintelligence and Human Intelligence Support to Joint Operations*.

f. JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*.

g. JP 2-03, *Geospatial Intelligence Support to Joint Operations*.

h. JP 3-0, *Joint Operations*.

i. JP 3-08, *Interagency Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations.*

j. JP 3-09, *Joint Fire Support*.

k. JP 3-13, *Information Operations*.

l. JP 3-16, *Multinational Operations*.

m. JP 3-33, *Joint Task Force Headquarters.*

n. JP 3-40, *Joint Doctrine for Combating Weapons of Mass Destruction.*

o. JP 5-0, *Joint Operation Planning*.

p. JP 6-0, *Joint Communications System*.

q. CJCSM 3500.04, *Universal Joint Task List*.

r. CJCS Message DTG 031640Z APR 06, *Joint Intelligence Operations Center (JIOC) Execute Order (EXORD)*.

APPENDIX D
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication to: Commander, United States Joint Forces Command, Joint Warfighting Center, ATTN: Doctrine Group, 116 Lake View Parkway, Suffolk, VA 23435-2697. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

The lead agent and Joint Staff doctrine sponsor for this publication is the Director for Intelligence (J-2).

3. Supersession

This publication supersedes JP 2-0, 9 March 2000, *Doctrine for Intelligence Support to Joint Operations*.

4. Change Recommendations

a. Recommendations for urgent changes to this publication should be submitted:

TO: CDRUSJFCOM SUFFOLK VA//DOC GP//
INFO: JOINT STAFF WASHINGTON DC//J7-JEDD//
JOINT STAFF WASHINGTON DC//J2//

Routine changes should be submitted electronically to Commander, Joint Warfighting Center, Doctrine and Education Group and info the Lead Agent and the Director for Operational Plans and Joint Force Development J-7/JEDD via the CJCS JEL at http://www.dtic.mil/doctrine.

b. When a Joint Staff directorate submits a proposal to the Chairman of the Joint Chiefs of Staff that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Military Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

c. Record of Changes:

CHANGE NUMBER	COPY NUMBER	DATE OF CHANGE	DATE ENTERED	POSTED BY	REMARKS

5. Distribution of Publications

Local reproduction is authorized and access to unclassified publications is unrestricted. However, access to and reproduction authorization for classified joint publications must be in accordance with DOD Regulation 5200.1-R, *Information Security Program*.

6. Distribution of Electronic Publications

a. Joint Staff J-7 will not print copies of JPs for distribution. Electronic versions are available on JDEIS at https://jdeis.js.mil (NIPRNET), and https://jdeis.js.smil.mil (SIPRNET) and on the JEL at http://www.dtic.mil/doctrine (NIPRNET).

b. Only approved joint publications and joint test publications are releasable outside the combatant commands, Services, and Joint Staff. Release of any classified joint publication to foreign governments or foreign nationals must be requested through the local embassy (Defense Attaché Office) to DIA Foreign Liaison Office, PO-FL, Room 1E811, 7400 Pentagon, Washington, DC 20301-7400.

c. CD-ROM. Upon request of a JDDC member, the Joint Staff J-7 will produce and deliver one CD-ROM with current joint publications.

GLOSSARY
PART I — ABBREVIATIONS AND ACRONYMS

AGI	advanced geospatial intelligence
AOR	area of responsibility
BDA	battle damage assessment
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CCDR	combatant commander
CCIR	commander's critical information requirement
CENTRIXS	Combined Enterprise Regional Information Exchange System
CI	counterintelligence
CIA	Central Intelligence Agency
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMO	civil-military operations
COA	course of action
COG	center of gravity
COM	collection operations management
COMINT	communications intelligence
CONOPS	concept of operations
CONPLAN	concept plan
COP	common operational picture
CPG	Contingency Planning Guidance
CRM	collection requirements management
CSS	Central Security Service
DFE	Defense Joint Intelligence Operations Center forward element
DIA	Defense Intelligence Agency
DIAP	Defense Intelligence Analysis Program
DJIOC	Defense Joint Intelligence Operations Center
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOS	Department of State
DTA	dynamic threat assessment
EEI	essential element of information
ELINT	electronic intelligence
EO	electro-optical
EXORD	execute order
FBI	Federal Bureau of Investigation

FISINT	foreign instrumentation signals intelligence
GEOINT	geospatial intelligence
GIG	Global Information Grid
GMI	general military intelligence
HSI	hyperspectral imagery
HUMINT	human intelligence
HVT	high-value target
I&W	indications and warning
IC	intelligence community
IGO	intergovernmental organization
IMINT	imagery intelligence
INSCOM	US Army Intelligence and Security Command
IO	information operations
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
J-2X	joint force staff counterintelligence and human intelligence element
J-3	operations directorate of a joint staff
J-5	plans directorate of a joint staff
J-6	communications system directorate of a joint staff
JCMB	Joint Collection Management Board
JDISS	joint deployable intelligence support system
JFC	joint force commander
JFCC-ISR	Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance
JIACG	joint interagency coordination group
JIOC	joint intelligence operations center
JIPOE	joint intelligence preparation of the operational environment
JISE	joint intelligence support element
JLLP	Joint Lessons Learned Program
JMD	joint manning document
JOA	joint operations area
JP	joint publication
JRIC	joint reserve intelligence center
JSCP	Joint Strategic Capabilities Plan
JTF	joint task force
JTL	joint target list
JWICS	Joint Worldwide Intelligence Communications System

LIDAR	light detection and ranging
LOC	line of communications
MASINT	measurement and signature intelligence
MCIA	Marine Corps Intelligence Activity
MEA	munitions effectiveness assessment
MEDINT	medical intelligence
MIB	Military Intelligence Board
MISREP	mission report
MOE	measure of effectiveness
MOP	measure of performance
MSI	multi-spectral imagery
NATO	North Atlantic Treaty Organization
NDP	national disclosure policy
NGA	National Geospatial-Intelligence Agency
NGO	nongovernmental organization
NIP	National Intelligence Program
NISP	national intelligence support plan
NIST	national intelligence support team
NMCC	National Military Command Center
NRO	National Reconnaissance Office
NSA	National Security Agency
NSL	no-strike list
OGA	other government agency
ONI	Office of Naval Intelligence
OPELINT	operational electronic intelligence
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PIR	priority intelligence requirement
PSYOP	psychological operations
QRT	quick reaction team
RFF	request for forces
RFI	request for information
RTL	restricted target list
S&T	scientific and technical
S&TI	scientific and technical intelligence

SCI	sensitive compartmented information
SIGINT	signals intelligence
SOF	special operations forces
TECHELINT	technical electronic intelligence
TECHINT	technical intelligence
TOPINT	technical operational intelligence
TSA	target system analysis
USCG	United States Coast Guard
USD(I)	Under Secretary of Defense (Intelligence)
USD(P)	Under Secretary of Defense (Policy)
USJFCOM	United States Joint Forces Command
USSTRATCOM	United States Strategic Command
WMD	weapons of mass destruction

PART II — TERMS AND DEFINITIONS

Unless otherwise annotated, this publication is the proponent for all terms and definitions found in the glossary. Upon approval, JP 1-02 will reflect this publication as the source document for these terms and definitions.

acoustic intelligence. Intelligence derived from the collection and processing of acoustic phenomena. Also called ACINT. (JP 2-0)

all-source intelligence. 1. Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence. 2. In intelligence collection, a phrase that indicates that in the satisfaction of intelligence requirements, all collection, processing, exploitation, and reporting systems and resources are identified for possible use and those most capable are tasked. See also intelligence. (JP 2-0)

analysis and production. In intelligence usage, the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of intelligence products in support of known or anticipated user requirements. (JP 2-01)

area of intelligence responsibility. None. (Approved for removal from the next edition of JP 1-02.)

area of interest. That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (JP 2-03)

asset (intelligence). Any resource — person, group, relationship, instrument, installation, or supply — at the disposition of an intelligence organization for use in an operational or support role. Often used with a qualifying term such as agent asset or propaganda asset. (JP 2-0)

biometric. Measurable physical characteristic or personal behavior trait used to recognize the identity or verify the claimed identity of an individual. (Approved for inclusion in the next edition of JP 1-02.)

biometrics. The process of recognizing an individual based on measurable anatomical, physiological, and behavioral characteristics. (Approved for inclusion in the next edition of JP 1-02.)

collate. 1. The grouping together of related items to provide a record of events and facilitate further processing. 2. To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing and exploitation portion of the intelligence process. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

collection. In intelligence usage, the acquisition of information and the provision of this information to processing elements. (JP 2-01)

collection management. In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. See also intelligence; intelligence process. (JP 2-0)

collection management authority. Within the Department of Defense, collection management authority constitutes the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. Also called CMA. (JP 2-01.2)

collection operations management. The authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and reporting resources. Also called COM. (JP 2-0)

collection planning. A continuous process that coordinates and integrates the efforts of all collection units and agencies. (JP 2-0)

collection requirements management. The authoritative development and control of collection, processing, exploitation, and/or reporting requirements that normally result in either the direct tasking of assets over which the collection manager has authority, or the generation of tasking requests to collection management authorities at a higher, lower, or lateral echelon to accomplish the collection mission. Also called CRM. (JP 2-0)

combat intelligence. That knowledge of the enemy, weather, and geographical features required by a commander in the planning and conduct of combat operations. (JP 2-0)

communications intelligence. Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called COMINT. (JP 2-0)

concept of intelligence operations. A verbal or graphic statement, in broad outline, of an intelligence directorate's assumptions or intent in regard to intelligence support of an operation or series of operations. The concept of intelligence operations, which supports the commander's concept of operations, is contained in the intelligence annex of operation plans. The concept of intelligence operations is designed to give an overall picture of intelligence support for joint operations. It is included primarily for additional clarity of

purpose. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

confirmation of information (intelligence). An information item is said to be confirmed when it is reported for the second time, preferably by another independent source whose reliability is considered when confirming information. (JP 2-0)

counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Also called CI. (JP 2-0)

critical intelligence. Intelligence that is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential or actual enemy. It includes but is not limited to the following: a. strong indications of the imminent outbreak of hostilities of any type (warning of attack); b. aggression of any nature against a friendly country; c. indications or use of chemical, biological, radiological, nuclear, or high-yield explosives weapons; and d. significant events within adversary countries that may lead to modifications of nuclear strike plans. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

current intelligence. One of two categories of descriptive intelligence that is concerned with describing the existing situation. (JP 2-0)

database. Information that is normally structured and indexed for user access and review. Databases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 2-0)

Department of Defense Intelligence Information System. The combination of Department of Defense personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national-level decision makers. Also called DODIIS. (JP 2-0)

Department of Defense Intelligence Information System Enterprise. The global set of resources (people, facilities, hardware, software and processes) that provide information technology and information management services to the military intelligence community through a tightly-integrated, interconnected and geographically distributed regional service center architecture. (Approved for inclusion in the next edition of JP 1-02.)

Department of Defense intelligence production. The integration, evaluation, analysis, and interpretation of information from single or multiple sources into finished intelligence for known or anticipated military and related national security consumer requirements. (This

term and its definition modify the existing term "defense intelligence production" and its definition and are approved for inclusion in the next edition of JP 1-02.)

dissemination and integration. In intelligence usage, the delivery of intelligence to users in a suitable form and the application of the intelligence to appropriate missions, tasks, and functions. (JP 2-01)

dynamic threat assessment. An intelligence assessment developed by the Defense Intelligence Agency that details the threat, capabilities, and intentions of adversaries in each of the priority plans in the Contingency Planning Guidance. Also called DTA. (Approved for inclusion in the next edition of JP 1-02.)

electro-optical intelligence. Intelligence other than signals intelligence derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far infrared (1,000 micrometers). Also called ELECTRO-OPTINT. See also intelligence; laser intelligence. (JP 2-0)

elicitation (intelligence). Acquisition of information from a person or group in a manner that does not disclose the intent of the interview or conversation. A technique of human source intelligence collection, generally overt, unless the collector is other than he or she purports to be. (JP 2-0)

enemy capabilities. Those courses of action of which the enemy is physically capable and that, if adopted, will affect accomplishment of the friendly mission. The term "capabilities" includes not only the general courses of action open to the enemy, such as attack, defense, reinforcement, or withdrawal, but also all the particular courses of action possible under each general course of action. "Enemy capabilities" are considered in the light of all known factors affecting military operations, including time, space, weather, terrain, and the strength and disposition of enemy forces. In strategic thinking, the capabilities of a nation represent the courses of action within the power of the nation for accomplishing its national objectives throughout the range of military operations. (JP 2-01.3)

essential elements of information. The most critical information requirements regarding the adversary and the environment needed by the commander by a particular time to relate with other available information and intelligence in order to assist in reaching a logical decision. Also called EEIs. (JP 2-0)

estimative intelligence. Intelligence that identifies, describes, and forecasts adversary capabilities and the implications for planning and executing military operations. (Approved for inclusion in the next edition of JP 1-02.)

evaluation and feedback. In intelligence usage, continuous assessment of intelligence operations throughout the intelligence process to ensure that the commander's intelligence requirements are being met. (JP 2-01)

foreign instrumentation signals intelligence. Technical information and intelligence derived from the intercept of foreign electromagnetic emissions associated with the testing and operational deployment of non-US aerospace, surface, and subsurface systems. Foreign instrumentation signals intelligence is a subcategory of signals intelligence. Foreign instrumentation signals include but are not limited to telemetry, beaconry, electronic interrogators, and video data links. Also called FISINT. See also signals intelligence. (JP 2-01)

foreign intelligence. Information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities. See also intelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

foundation data. Specific information on essential features that change rarely or slowly, such as point positioning data, topographic features, elevation data, geodetic information, and safety of navigation data. (JP 2-03)

fusion. In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 2-0)

fusion center. None. (Approved for removal from the next edition of JP 1-02.)

general military intelligence. Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or multinational military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries; military and civilian communications systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) Also called GMI. See also intelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

geospatial information. Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including: statistical data and information derived from, among other things, remote sensing, mapping, and surveying technologies; and mapping, charting, geodetic data and related products. (JP 2-03)

geospatial information and services. The collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately

referenced to a precise location on the Earth's surface. Geospatial services include tools that enable users to access and manipulate data, and also include instruction, training, laboratory support, and guidance for the use of geospatial data. Also called GI&S. (JP 2-03)

geospatial intelligence. The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. Also called GEOINT. (JP 2-03)

human factors. The psychological, cultural, behavioral, and other human attributes that influence decision-making, the flow of information, and the interpretation of information by individuals or groups. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

human intelligence. A category of intelligence derived from information collected and provided by human sources. Also called HUMINT. (JP 2-0)

imagery intelligence. The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. Also called IMINT. See also intelligence. (JP 2-03)

indications. In intelligence usage, information in various degrees of evaluation, all of which bear on the intention of a potential enemy to adopt or reject a course of action. (This term and its definition modify the existing term "indications (intelligence)" and its definition and are approved for inclusion in the next edition of JP 1-02.)

indications and warning. Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to US citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied and/or coalition nations. Also called I&W. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

indicator. In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

information requirements. In intelligence usage, those items of information regarding the adversary and other relevant aspects of the operational environment that need to be collected and processed in order to meet the intelligence requirements of a commander. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence community. All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called IC. (JP 2-01.2)

intelligence discipline. A well defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. There are seven major disciplines: human intelligence, geospatial intelligence, measurement and signature intelligence, signals intelligence, open-source intelligence, technical intelligence, and counterintelligence. See also human intelligence; geospatial intelligence; measurement and signature intelligence; signals intelligence; open-source intelligence; technical intelligence; counterintelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence estimate. The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence federation. A formal agreement in which a combatant command joint intelligence center receives preplanned intelligence support from other joint intelligence centers, Service intelligence organizations, Reserve organizations, and national agencies during crisis or contingency operations. (JP 2-01)

intelligence operations. The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. Intelligence operations include planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 2-01)

intelligence process. The process by which information is converted into intelligence and made available to users. The process consists of six interrelated intelligence operations: planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback. (JP 2-01)

intelligence requirement. 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces.

(This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

intelligence source. The means or system that can be used to observe and record information relating to the condition, situation, or activities of a targeted location, organization, or individual. An intelligence source can be people, documents, equipment, or technical sensors. (JP 2-0)

intelligence, surveillance, and reconnaissance. An activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. Also called ISR. (JP 2-01)

intelligence, surveillance, and reconnaissance visualization. The capability to graphically display the current and future locations of intelligence, surveillance, and reconnaissance sensors, their projected platform tracks, vulnerability to threat capabilities and meteorological and oceanographic phenomena, fields of regard, tasked collection targets, and products to provide a basis for dynamic re-tasking and time-sensitive decision making. Also called ISR visualization. (JP 2-01)

intention. An aim or design (as distinct from capability) to execute a specified course of action. (JP 2-01)

interpretation. A part of the analysis and production phase in the intelligence process in which the significance of information is judged in relation to the current body of knowledge. (JP 2-01)

joint captured materiel exploitation center. A physical location for deriving intelligence information from captured enemy materiel. It is normally subordinate to the joint force/J-2. Also called JCMEC. (JP 2-01)

joint deployable intelligence support system. A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (JP 2-0)

joint document exploitation center. A physical location for deriving intelligence information from captured adversary documents including all forms of electronic data and other forms of stored textual and graphic information. It is normally subordinate to the joint force/J-2. Also called JDEC. See also intelligence. (JP 2-01)

joint intelligence. Intelligence produced by elements of more than one Service of the same nation. (JP 2-0)

joint intelligence architecture. A dynamic, flexible structure that consists of the Defense Joint Intelligence Operations Center, combatant command joint intelligence operations centers, and subordinate joint task force intelligence operations centers or joint intelligence support elements. This architecture

encompasses automated data processing equipment capabilities, communications and information requirements, and responsibilities to provide national, theater, and tactical commanders with the full range of intelligence required for planning and conducting operations. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

joint intelligence center. None. (Approved for removal from the next edition of JP 1-02.)

joint intelligence operations center. An interdependent, operational intelligence organization at the Department of Defense, combatant command, or joint task force (if established) level, that is integrated with national intelligence centers, and capable of accessing all sources of intelligence impacting military operations planning, execution, and assessment. Also called JIOC. (Approved for inclusion in the next edition of JP 1-02.)

joint intelligence preparation of the operational environment. The analytical process used by joint intelligence organizations to produce intelligence assessments, estimates and other intelligence products in support of the joint force commander's decision making process. It is a continuous process that includes defining the operational environment; describing the effects of the operational environment; evaluating the adversary; and determining and describing adversary potential courses of action. Also called JIPOE. (This term and its definition are provided for information and are proposed for inclusion in the next edition of JP 1-02 by JP 2-01.3.)

joint intelligence support element. A subordinate joint force element whose focus is on intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (JP 2-01)

Joint Worldwide Intelligence Communications System. The sensitive compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 2-0)

laser intelligence. Technical and geo-location intelligence derived from laser systems; a subcategory of electro-optical intelligence. Also called LASINT. See also electro-optical intelligence; intelligence. (JP 2-0)

measurement and signature intelligence. Intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted. Also called MASINT. See also intelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

medical intelligence. That category of intelligence resulting from collection, evaluation, analysis, and interpretation of foreign medical, bio-scientific, and environmental information that is of interest to strategic planning and to military medical planning and operations for the conservation of the fighting strength of friendly forces and the formation of assessments of foreign medical capabilities in both military and civilian sectors. Also called MEDINT. See also intelligence. (JP 2-01)

Military Intelligence Board. A decision-making forum which formulates Department of Defense intelligence policy and programming priorities. Also called MIB. See also intelligence. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

national intelligence. The terms "national intelligence" and "intelligence related to the national security" each refers to all intelligence, regardless of the source from which derived and including information gathered within or outside of the United States, which pertains, as determined consistent with any guidelines issued by the President, to the interests of more than one department or agency of the Government; and that involves (a) threats to the United States, its people, property, or interests; (b) the development, proliferation, or use of weapons of mass destruction; or (c) any other matter bearing on United States national or homeland security. (JP 2-01.2)

national intelligence support team. A nationally sourced team composed of intelligence and communications experts from Defense Intelligence Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, or other intelligence community agencies as required. Also called NIST. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

National Military Joint Intelligence Center. None. (Approved for removal from the next edition of JP 1-02.)

nuclear intelligence. Intelligence derived from the collection and analysis of radiation and other effects resulting from radioactive sources. Also called NUCINT. See also intelligence. (JP 2-0)

obstacle intelligence. Those collection efforts to detect the presence of enemy (and natural) obstacles, determine their types and dimensions, and provide the necessary information to plan appropriate combined arms breaching, clearance, or bypass operations to negate the impact on the friendly scheme of maneuver. It is typically related to the tactical level of intelligence. Also called OBSTINTEL. (Approved for inclusion in the next edition of JP 1-02.)

open-source intelligence. Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 2-0)

operational intelligence. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or operational areas. (JP 2-0)

persistent surveillance. A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and retargeting in near or real-time. Persistent surveillance facilitates the prediction of an adversary's behavior and the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

planning and direction. In intelligence usage, the determination of intelligence requirements, development of appropriate intelligence architecture, preparation of a collection plan, and issuance of orders and requests to information collection agencies. (JP 2-01)

priority intelligence requirement. An intelligence requirement, stated as a priority for intelligence support, that the commander and staff need to understand the adversary or the operational environment. Also called PIR. (JP 2-0)

processing and exploitation. In intelligence usage, the conversion of collected information into forms suitable to the production of intelligence. (JP 2-01)

radar intelligence. Intelligence derived from data collected by radar. Also called RADINT. See also intelligence. (JP 2-0)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. Also called RECON. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

red team. An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the perspective of adversaries and others. (Approved for inclusion in the next edition of JP 1-02.)

request for information. 1. Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the combatant command's procedures. 2. The National Security Agency/Central Security Service uses this term to state ad hoc signals intelligence requirements. Also called RFI. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

scientific and technical intelligence. The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information that covers: a. foreign developments in basic and applied research and in applied engineering techniques; and b. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel; the research and development related thereto; and the production methods employed for their manufacture. Also called S&TI. (JP 2-01)

signals intelligence. 1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted. 2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called SIGINT. See also communications intelligence; foreign instrumentation signals intelligence; intelligence. (JP 2-0)

strategic intelligence. Intelligence required for the formation of policy and military plans at national and international levels. Strategic intelligence and tactical intelligence differ primarily in level of application, but may also vary in terms of scope and detail. See also intelligence; operational intelligence; tactical intelligence. (JP 2-01.2)

synchronization. 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan to ensure intelligence requirements are answered in time to influence the decisions they support. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

tactical intelligence. Intelligence required for the planning and conduct of tactical operations. See also intelligence. (JP 2-01.2)

tear line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release. (JP 2-0)

technical intelligence. Intelligence derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages. Also called TECHINT. (This term and its definition modify the existing term and its definition and are approved for inclusion in the next edition of JP 1-02.)

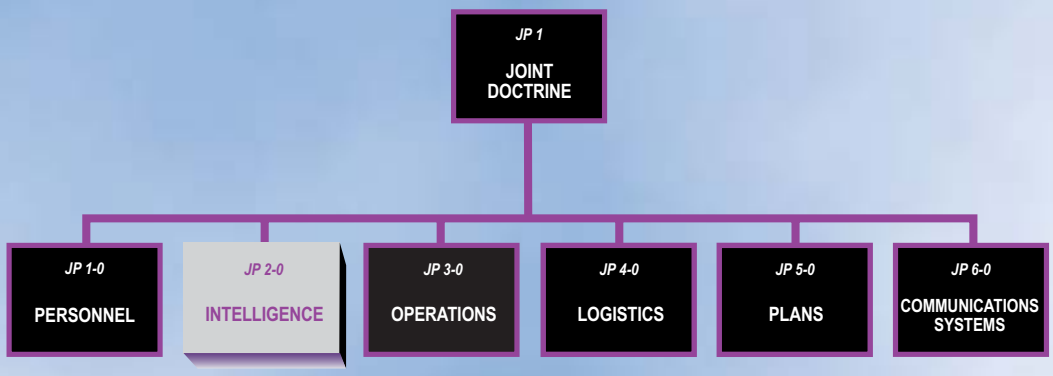
threat warning. The urgent communication and acknowledgement of time-critical information essential for the preservation of life and/or vital resources. (JP 2-01)

validation. 1. A process associated with the collection and production of intelligence that confirms that an intelligence collection or production requirement is sufficiently important to justify the dedication

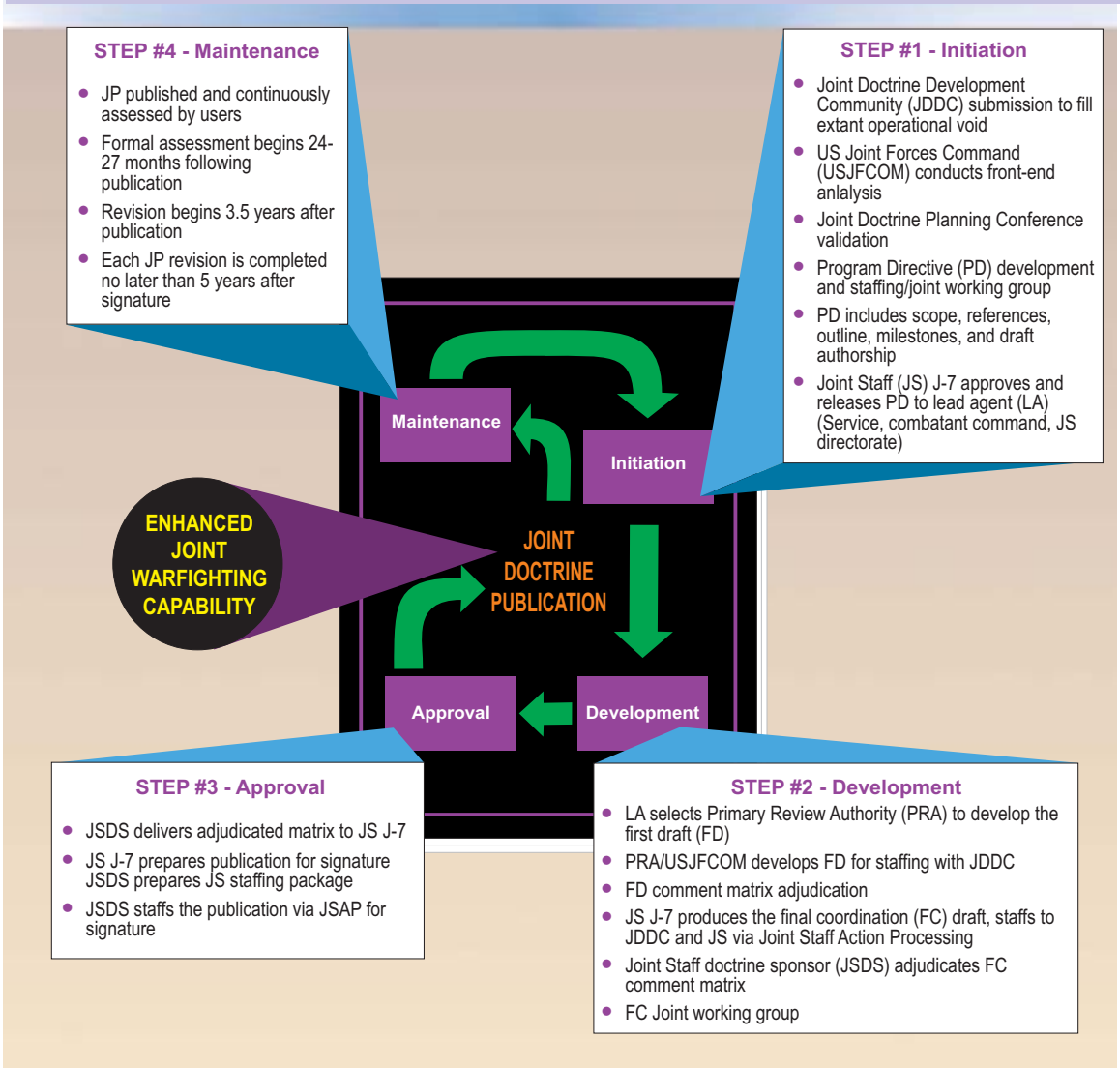
of intelligence resources, does not duplicate an existing requirement, and has not been previously satisfied. 2. A part of target development that ensures all vetted targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of armed conflict and rules of engagement. 3. In computer modeling and simulation, the process of determining the degree to which a model or simulation is an accurate representation of the real world from the perspective of the intended uses of the model or simulation. 4. Execution procedure used by combatant command components, supporting combatant commanders, and providing organizations to confirm to the supported commander and United States Transportation Command that all the information records in a time-phased force and deployment data not only are error free for automation purposes, but also accurately reflect the current status, attributes, and availability of units and requirements. (JP 3-35)

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 2-0** is in the **Intelligence** series of joint doctrine publications. The diagram below illustrates an overview of the development process:




JOINT
CHIEFS OF STAFF